# Estructuració de xarxes. Disseny i implementació de serveis a Instituts d'Educació Secundaria.

Tutor : Enric Guitart Baraut
Per : Rubén Artacho Cortada

2 de juliol de 2008

# Agraïments

Gracies...

...als responsables de l'IES Joan Oró de Lleida per haver cedit les seves instal·lacions per a obtenir la informació necessària per a la realització d'aquest projecte.

...a Artur Guillaumet coordinador d'informàtica de l'IES Gili i Gaya de Lleida per compartir amb mi les seves experiències sobre la gestió de les TIC en un centre de secundària.

... a Enric Guitart per les seves orientacions i per dirigir aquest projecte.

... a Verònica, pel seu recolzament incondicional.

# Índex

# Índex de figures

# Índex de taules

# Capítol 1

# Pròleg

Després de dos anys mantenint els sistemes informàtics de varis Instituts d'Educació Secundària (IES)de la ciutat de Lleida s'ha aconseguit obtenir la informació suficient per a definir amb precisió els problemes i l'estat dels sistemes informàtics que per norma general presenten molts IES tant de la ciutat de Lleida com de la resta de la província.

Moltes de les incidències que es donen als IES són evitables configurant adequadament el sistema.

La idea , és dissenyar un sistema informàtic fàcilment adaptable a qualsevol IES i sobre aquesta premissa es construirà aquest projecte.

# Part I

# Memòria

# Capítol 2

# Introducció

Amb el creixement de les noves tecnologies i en especial de les tecnologies de la informació i la comunicació, en endavant TIC, els centres educatius evolucionen cap a noves formes i tècniques d'ensenyament. Encara que continua essent vigent el clàssic mètode de la pissarra, el llibre i la llibreta, cada cop més les TIC ofereixen un ampli ventall de noves possibilitats per complementar i ampliar els conceptes i les informacions vistes a classe i elaborar continguts. En definitiva les TIC poden arribar a ésser una eina útil i poderosa per a l'ensenyament i la formació del jovent.

Les TIC però s'enfronten a nous reptes per ésser utilitzades de forma generalitzada en l'ensenyament, en primer lloc han de complir una serie de requisits. Cal que les estacions, la xarxa i els serveis que aquesta ofereix es comportin com s'espera, ja que en cas contrari es pot produir una situació en la qual els usuaris poden sofrir molèsties, la qual cosa pot comportar que les aules TIC caiguin en desús. També es important que els equips d'usuari siguin fàcils d'utilitzar, protegir adequadament les dades d'usuari, que el manteniment del sistema sencer sigui senzill i poc costós, i que la resposta davant les fallides sigui ràpida i que aquestes no provoquin pèrdues irreversibles de dades.

A mes amb la introducció d'Internet a les aules s'obre tot un món d'informació i coneixement a l'abast de la comunitat educativa. Internet però avui en dia es un territori salvatge i hostil , les xarxes connectades a Internet són amenaçades per virus i altres tipus de programari malintencionat, per intrusos maliciosos i a més, essent el cas d'un centre educatiu, cal gestionar adequadament els continguts per evitar que aquells restringits per adults o que posin en perill la dinàmica de les classes siguin accessibles des del centre.

D'aquesta manera les TIC poden ésser usades en un centre educatiu de forma segura i amb garanties que seran una eina útil en l'ensenyament secundari.

L'objectiu d'aquest projecte es donar solució als problemes esmentats, dissenyar i implementar tant la xarxa del centre com els serveis que ha d'oferir de forma que compleixi els requeriments anteriors.

# Capítol 3

# Estat actual del centre

## 3.1 Xarxa física

La xarxa del centre es composa d'una única LAN (*Local Area Network*) de tipus Ethernet cablejada mitjançant cable UTP (*Unshielded Twisted Pair*) de categoria 5e, a l'hora de crear la xarxa actual no es va seguir cap tipus d'estructuració sinó que es va ampliar conforme a les necessitats immediates.

La xarxa està formada per equips de tipus switch no gestionables, la majoria no instal·lats en armaris de comunicacions.

L'actual configuració ha donat múltiples problemes de connectivitat i de denegació de serveis, a més de no ser una configuració segura, ja que permet l'accés a ordinadors clau com els de direcció, secretaria i professorat des dels equips d'alumnes.

## 3.2 Serveis

Els serveis que atorga la xarxa són bàsicament dos:

- Internet : La connexió de la xarxa del centre a Internet es fa mitjançant un router ADSL (*Asymetric Digital Subscriber Line*) 256Kbps/3-8 Mbps Cisco serie 800. Aquestos equips fan servir NAT (*Network Address Translation*) per connectar tots els equips del centre a través d'una única adreça IP pública. Aquesta configuració permet una certa protecció dels equips de la xarxa interna ja que aquestos no son accessibles directament des de Internet.

- Serveis d'arxius : Consta d'un espai comú per a tot el centre i d'alguns espais compartits pels professors. Tampoc hi ha cap tipus d'autenticació personal dels usuaris i com a conseqüència no hi han espais

personals de disc. Per fer servir les estacions, es fan servir tres comptes d'usuari. Aquestos son :

1. Alum-01 : Compte d'usuari per alumnes.
2. Prof : Compte d'usuari per professors.
3. Super : Compte de l'administrador.

## 3.3 Estacions de treball

Les estacions de treball són majoritariament equips PC compatibles que corren el sistema operatiu Microsoft Windows XP. En ocasions es poden trobar també màquines amb el sistema operatiu MacOSX. I rarament alguna amb sistema operatiu Linux.

## 3.4 Problemes més freqüents als IES.

En aquest apartat s'enumeren els problemes que amb més freqüència es presenten als IES, aquestos son problemes que han provocat incidències de manteniment en centres de secundària durant els últims dos anys :

- Pèrdua de dades : S'han donat casos de pèrdua de dades deguts a fallides de hardware. A més, com molts dels espais comuns de dades estan oberts a tothom, hi han hagut casos també de pèrdua o modificació maliciosa de dades.
- Falta de control d'accés : Les contrasenyes freqüentment es troben apuntades en la pantalla de cada estació.
- Denegació de servei : S'han donat casos de fallides del sistema degudes a manipulacions negligents o malicioses de la xarxa (creació de bucles a la xarxa Ethernet, desconnexió d'equips i d'altres).
- Accés a continguts no apropiats : S'han donat casos en els que alumnes accedeixen durant les classes a Internet a continguts no apropiats per la seva edat i/o continguts lúdics que afecten greument la dinàmica de les classes.
- Lentitud en l'accés a Internet : La gran quantitat d'equips i d'usuaris que fan servir Internet unit a que només es disposen de 4 Mbps de velocitat de connexió fan que a determinades hores del dia els serveis

d'Internet pateixin una forta degradació del rendiment. A més la proliferació a la xarxa d'equips amb programes de tipus Peer to Peer encara fa més greu el problema. També s'aprecia un forta redundància en les peticions a Internet, quasi sempre totes les estacions d'una aula accedeixen a les mateixes pàgines i descarreguen els mateixos arxius.

- Equips d'administració i de professors accessibles des d'equips d'alumnes : Aquest problema es inherent a la pròpia estructura de la xarxa, només una xarxa Ethernet per a tot el centre. Tots els equips poden connectar uns amb els altres. Si algun equip amb dades importants no es troba correctament protegit pot ser atacat fàcilment.

- Servidors privatius : Alguns centres fan servir sistemes privatius pels servidors, la qual cosa fa difícil escalar aquestos o integrar-los fàcilment amb altres sistemes. A més el cost de llicència del software i de les llicències d'accés per client suposa una despesa innecessària.

# Capítol 4

# Estudi previ

## 4.1 Determinació de les causes dels problemes

La causa fonamental dels problemes esmentats es que els sistemes informàtics que actualment es poden trobar als centres no implementen per norma general cap tipus de control d'accés personalitzat, no es controla el trànsit de la xarxa i la electrònica de xarxa es fàcilment accessible. Aquesta manca de control sobre els recursos TIC dels centres esta provocant incidències que serien evitables amb una configuració estudiada de la xarxa i dels serveis.

A continuació es tractarà d'establir alguns dels objectius que es pretenen aconseguir amb aquest treball.

## 4.2 Objectius

El principal objectiu d'aquest projecte es donar solucions per tal de pal·liar o eliminar els problemes esmentats amb anterioritat. Es passa a considerar els objectius amb més detall.

1. Privacitat i pèrdua de dades : Les dades tant d'alumnes com de professors i PAS (*Personal Administració i Serveis*) han de ser personals. Cada usuari hauria de tenir només accés a les seves dades i a les dades publiques que el centre consideri convenient. Cal també posar mitjans per evitar que fallides de maquinari provoquin pèrdues de dades.

2. Control d'accés : S'han de proporcionar mecanismes per identificar els usuaris i definir quin grau d'accés a les diferents parts del sistema i quin accés a les dades tindran.

3. Estabilitat de servei : Tant la xarxa com els serveis han d'estar disponibles i ser tolerants a fallides. Cal restringir l'accés al cablejat de la xarxa.

4. Accés a continguts no apropiats : Es important garantir al centre el control sobre els continguts que els alumnes podran visualitzar des de Internet. També ho és guardar un històric de les pàgines visitades per comprovar-les i restringir-les si s'escau.

5. Lentitud d'accés a Internet : Els accessos redundants a informació d'Internet han de ser eliminats ja que no són productius. No té sentit descarregar una còpia del mateix arxiu per cada estació de treball de l'aula. S'eliminarà selectivament el tràfic P2P (*Peer To Peer*). Aquestes mesures haurien de provocar una notable millora en la velocitat d'accés a continguts d'Internet.

6. Separació de la xarxa : Cal protegir i aïllar adequadament les xarxes a les que es connecten els equips de professorat i PAS. S'han d'evitar accessos no autoritzats des d'altres xarxes del centre i des de Internet.

7. Manteniment : Seria desitjable que el manteniment del sistema sigui senzill i poc costós.

8. Viabilitat : El sistema dissenyat ha de ser viable econòmica i legalment. La finalitat es aconseguir un producte de baix cost, amb bona funcionalitat i que pugui ser implantat en un centre real.

## 4.3 Proposta de solució.

Es proposen les següents actuacions per tal de reduir o evitar la incidència dels problemes esmentats.

En primer lloc cal dir que per mantenir la compatibilitat amb els serveis i el hardware existent es proposa implementar una xarxa TCP/IP sobre Ethernet i implementar els serveis sobre aquesta. Per separar d'alguna manera les actuacions a realitzar s'ha divisdit l'anàlisi del sistema en dues parts : La xarxa i els serveis de xarxa.

Aquesta separació es fa en base a les diferents capes de les que consta l'arquitectura de la xarxa emprada.

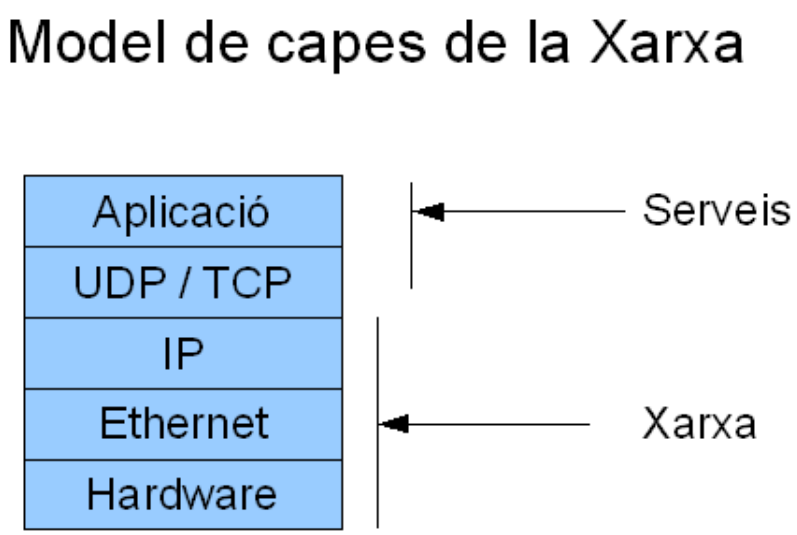



Figura 4.1: Model capes de xarxa

A la figura 4.1 es pot veure gràficament quines capes tenen papers rellevants en cadascuna de les dues parts en que es separa el nostre sistema.

### 4.3.1 Xarxa

Cal introduir algunes millores en la xarxa ,aquestes es detallen a continuació :

1. Cablejat estructurat de la xarxa Ethernet : Cablejant correctament la xarxa i tancant els equips en armaris de 19 polzades, s'aconsegueix una millor estructuració i protecció de la xarxa.

2. Separació a nivell 2 de la xarxa mitjançant VLANs : Es necessari separar els diferents departaments a nivell 2 per evitar l'accés directe entre equips de diferents departaments.

3. Utilització de Spanning Tree i d'enllaços redundats : Aquesta mesura protegirà contra bucles en la xarxa i minimitzarà l'impacte de la caiguda d'un equip o d'un enllaç.

4. Sistemes d'alimentació ininterrompuda : La instal·lació d'aquest tipus d'equipament donarà protecció contra interrupcions o fluctuacions del corrent elèctric.

5. Complement WI-FI : Es contempla ampliar la xarxa local mitjançant la utilització de punts d'accés sense fils.

6. Encaminament a nivell 3 de la xarxa : És necessari encaminar el tràfic per poder donar accés als serveis que ofereix la xarxa als diferents departaments.

7. Llistes de control d'accés a nivell 3 de la xarxa : S'ha de restringir les comunicacions entre departaments i sobretot protegir departaments especialment sensibles.

8. Maquinari necessari :Tots aquests serveis son implementables gràcies al Projecte Heura del Departament d'Ensenyament, que ha destinat fons al cablejat de les escoles i a l'adquisició d'equips de xarxa. Aquestos equips consten de:

- Switch/Router Zyxel GS-4024 (amb capacitat de commutació a nivell 3 , ACL's (*Acces Control Lists*), 802.1q, RSTP (*Rapid Spanning Tree Protocol*)).

- Punts d'accés DLink DWL-2200AP (suporta RADIUS (*Remote Authentication Dial In User Service*), 802.1q, WPA,MulitSSID (*Multiple Service Set Identifier*)).

- Un o més switches Zyxel ES-2024 (802.1q,RSTP).

El Projecte Heura s'instal·la amb una configuració per defecte que haurà de ser modificada per adaptar-la a les necessitats d'estructuració de xarxa i les aplicacions.

### 4.3.2 Serveis de la xarxa

Es configuraran els següents serveis :

1. Servei d'autenticació centralitzada : Es crearà una base de dades d'usuaris del centre distingint entre professors i alumnes. S'emprarà una o més aplicacions per validar els usuaris a les estacions. La única excepció a aquesta regla son els ordinadors de l'equip directiu i PAS, aquestos per considerar-se personals i intransferibles s'autentifiquen localment i resten aïllats de la resta de la xarxa, només tenen accés a Internet a través de NAT.

2. Servei de Proxy i Caché : S'implementarà un servei de Proxy transparent el qual disposarà d'una Caché de disc que servirà per millorar la velocitat d'accés a Internet.

3. Gestió de continguts web: S'afegirà també programari per controlar els accessos a Internet , aquest permetrà veure estadístiques anònimes dels accessos a Internet i els dominis visitats, a més de proporcionar mitjans per restringir la visualització de certes pàgines o de dominis sencers.

4. Servei d'emmagatzematge de dades : S'haurà de crear múltiples espais de dades, tant personals com comunitaris. Aquestos es trobaran en un o més servidors centralitzats que implementin mecanismes de protecció de dades adequats, tant a nivell de maquinari com de programari. Haurà d'establir-se una política de copies de seguretat periòdiques per evitar pèrdues de dades.

5. Filtrat a nivell d'aplicació : Caldrà eliminar selectivament tràfic no desitjat o que pugui saturar la xarxa, programes P2P, MSN Messenger (missatgeria instantània), chat, etc.

6. Sistemes d'alimentació ininterrompuda : La instal·lació d'aquest tipus d'equipament donarà protecció contra interrupcions o fluctuacions del corrent elèctric.

### 4.3.3 Maquinari necessari

Es necessitaran al menys tres equips de propòsit general. Pel seu baix cost i bones prestacions s'escolleixen màquines compatibles intel. S'implementarà l'emmagatzemament mitjançant RAID (*Redundant Array of Independent Discs*) per dotar de redundància de dades i una certa tolerància a fallides.

### 4.3.4 Programari necessari

Es mantindrà el programari de les estacions de treball per evitar molèsties als usuaris. El programari de servidor en canvi es substituirà íntegrament per programari lliure. D'aquesta manera s'obtindrà un bon funcionament, millor escalabilitat, menor cost i millor integració amb altres tipus de estacions.

### 4.3.5 Pla de Manteniment

Per a facilitar el manteniment i la implantació del sistema caldrà tenir algunes consideracions a l'hora de dissenyar el sistema.

1. Us d'estàndards : Cal evitar en la mesura del possible haver d'instal·lar software addicional per a implementar el sistema. Sempre que es pugui caldrà fer servir els protocols d'aplicació estàndard de cada sistema operatiu per a la implementació de serveis.

2. Configuració de les estacions : És necessari reduir i documentar els passos a seguir per configurar les estacions de treball, aquesta configuració haurà de ser senzilla i ràpida.

3. Documentació de l'usuari : S'ha d'elaborar manuals que descriguin el procés de configuració i implantació del sistema.

4. Copies de seguretat : Caldrà establir una política de còpies de seguretat adequada per tal de reduir la possibilitat de pèrdua de dades.

5. Revisió de continguts : S'ha de revisar quins continguts d'Internet són accedits i poder denegar l'accés a aquestos si s'escau.

6. Programes auxiliars : S'elaboraran programes que automatitzin les tasques més feixugues o tècnicament difícils.

## 4.4 Expectatives de compliment dels objectius

1. Privacitat de dades : S'espera que amb les actuacions proposades s'aconsegueixi una major privacitat de dades, gràcies a les restriccions de les comunicacions, la separació dels espais de dades i el control d'accés individualitzat.

2. Pèrdua de dades : Es d'esperar que la centralització de les dades, la utilització de tecnologies RAID, el control d'accés i una bona política de copies de seguretat redueixin en gran mesura la possibilitat de pèrdues de dades accidentals o malintencionades.

3. Control d'accés : Mitjançant els serveis d'accés centralitzat, filtrat a nivell d'aplicació, gestió de continguts i les restriccions imposades a les comunicacions s'obtindrà un major grau de control sobre l'accés als serveis, a les dades, a la xarxa i als continguts que aquesta ofereix.

4. Estabilitat de servei : Un cop s'hagi restringit mitjançant armaris l'accés al cablejat de la xarxa i s'habiliti el protocol de Spanning Tree es pot aconseguir una certa protecció a manipulacions de la xarxa ( creació de bucles, desconnexió d'equips). La contrapartida de la instal·lació

es que es vulnerable a la fallida del switch/router central. S'han instal·lat sistemes d'alimentació ininterrompuda per minimitzar fallides de la xarxa i enllaços redundants entre armaris per a aconseguir que la caiguda d'un dels switch secundaris no provoqui la caiguda de l'enllaç.

5. Accés a continguts no apropiats : Es de preveure que la posada en marxa d'un Proxy amb capacitats de filtrat de continguts i l'eliminació de determinats tipus de tràfic dificultin l'accés a continguts no lectius.

6. Lentitud d'accés a Internet : La utilització de proxys i la eliminació de programes P2P haurien de produir un notable augment de la velocitat d'aplicacions HTTP (*Hyper Text Transfer Protocol*).

7. Separació de la xarxa : Mitjançant 802.1q, VLANs i filtrat de tràfic IP s'aconsegueix aïllar els ordinadors entre departaments.

8. Viabilitat : Caldrà optar per tecnologies amb baix cost econòmic. Es necessari també simplificar i minimitzar els processos d'implantació i de manteniment.

## 4.5 Planificació temporal del projecte

El projecte es comença en setembre de 2007 i hauria d'estar finalitzat el juny de 2008. El nombre d'hores diàries de treball és de 2, per motius de treball.

S'han estructurat les tasques a fer en les següents:

1. Estudi estat actual : Concretar els problemes que s'han de resoldre i definir possibles solucions.

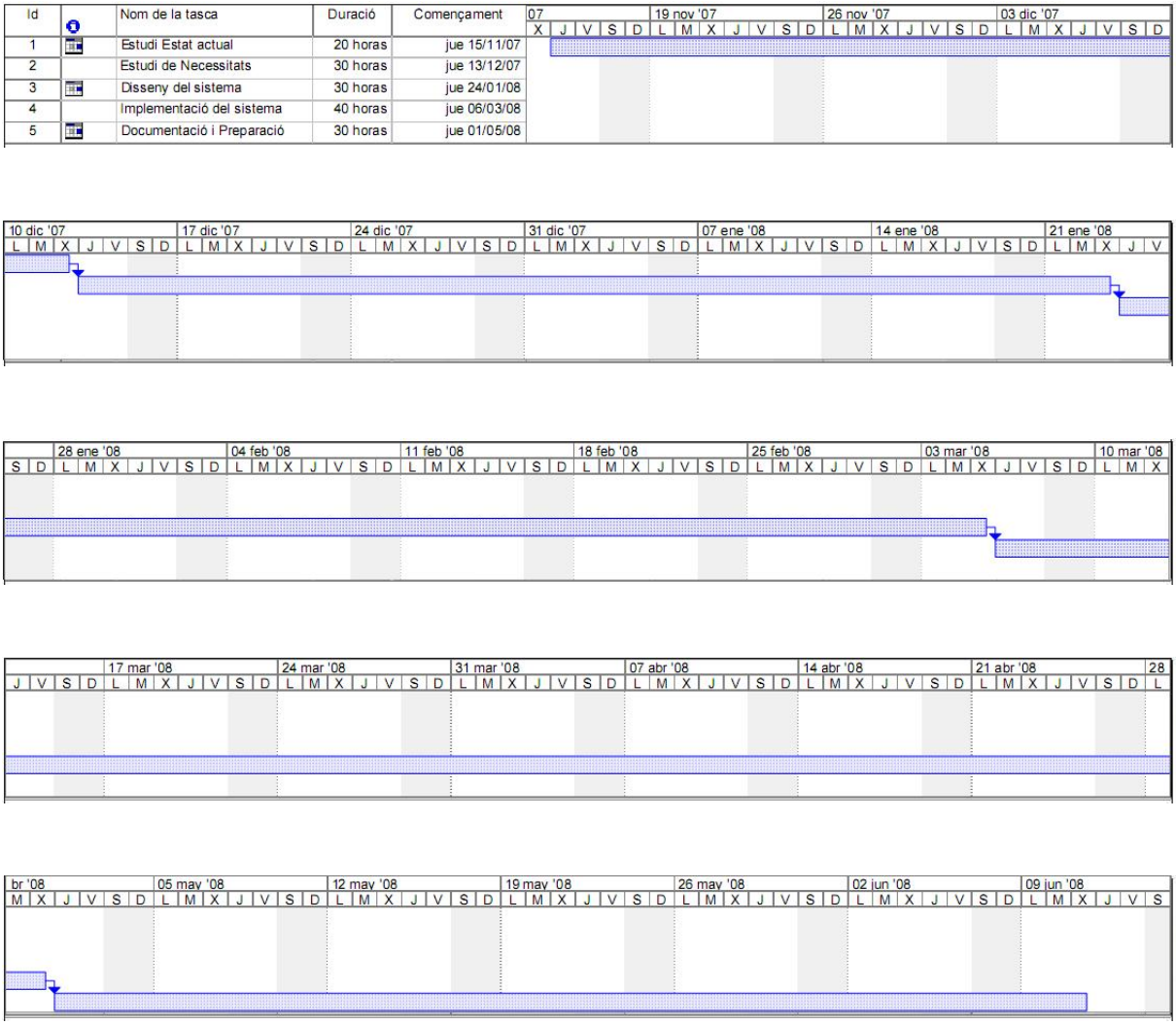
2. Estudi de necessitats : Estudiar detingudament les solucions als problemes dels centres i definir els punts forts i febles de les aplicacions que es poden utilitzar per implementar les solucions. Escollir les aplicacions més aptes.

3. Disseny del sistema : Detallar la configuració de les aplicacions que formaran el sistema. Definir la estructura de la xarxa.

4. Implementació del sistema : Crear el programa de configuració dels switch. Implementar els servidors sobre màquines virtuals. Fer proves de funcionament de la xarxa i els serveis.

5. Documentació i preparació : Documentar tot el treball. Escriure la memòria, la pressentació i crear els arxius de suport.

Al diagrama de Gant següent es poden veure les fases del projecte, la seva duració i precedència.



# Capítol 5

# Especificació i disseny del sistema

A continuació es detallen les decisions de disseny que s'hauran de tenir en compte a la fase d'implementació. S'ha procurat mantenir la funcionalitat actual del sistema al màxim per mantenir una adequada usabilitat d'aquest. Es farà tot el possible per mantenir els actuals serveis. El funcionament i les interfícies actuals de les estacions de treball s'hauran de mantenir en la mesura del possible. Es a dir, la migració del sistema haurà de ser tan transparent al usuari com sigui possible.

Al capítol de la implementació es podrà veure amb més detall totes les configuracions i el disseny final dels sistemes implementats.

## 5.1 Xarxa

La xarxa és la que proporciona el Projecte Heura . Aquest projecte dotarà de cablejat estructurat als centres educatius públics.

Tot seguit es detallen algunes de les característiques més importants de les instal·lacions :

- Es cablejaran els centres amb cable UTP de categoria 6 dins de canalitzacions de PVC.
- Es fan servir un armari o rack principal i opcionalment un o més de secundaris.
- La connexió entre armaris és redundant, es fan servir 2 enllaços.

A la figura 5.1 es pot veure l'esquema de connexionat entre armaris.

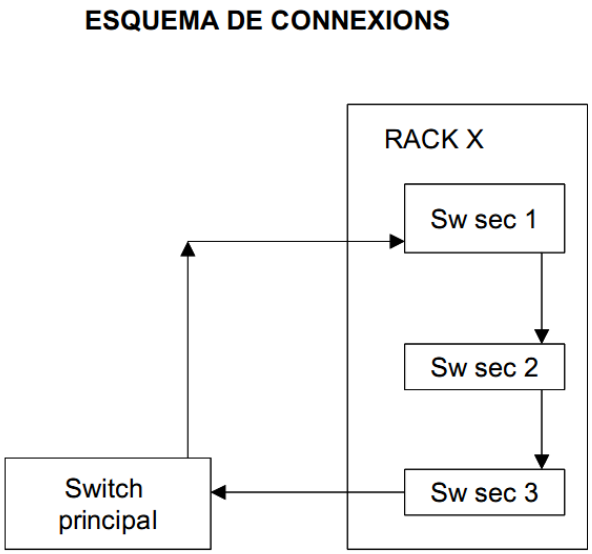



Figura 5.1: Connexionat entre armaris

- A l'armari principal s'instal·larà com a mínim un switch Zyxel GS-4024 amb capacitat de commutació a nivell 3, i un SAI Riello 1500 V.A. gestionable via SNMP (*Simple Network Management Protocol*), a més també es poden instal·lar opcionalment un o varis switch Zyxel ES-2024 (sense capacitat de routing) i equips PoE (*Power over Ethernet*) per a l'alimentació dels punts d'accés sense fils.

- Als armaris secundaris només hi haurà un o varis switch Zyxel ES-2024 i equips PoE per a l'alimentació dels punts d'accés sense fils.

### 5.1.1 Cablejat

A mode il·lustratiu a la figura 5.2 i 5.3 es mostra el cablejat d'un centre de secundària. En aquest cas els plànols corresponen a un IES de la província de Lleida. Als plànols adjunts es pot veure detalladament la situació dels armaris de comunicacions i del recorregut dels cables UTP, també la localització dels punts d'accés sense fils i la seva cobertura mesurada amb l'aparell WiNet. Les zones de cobertura són aquelles en les que la relació senyal/soroll es de com a mínim -76dBm, que segons el fabricant correspon a una velocitat de 36 Mbps que es la velocitat mínima que demana el Departament.

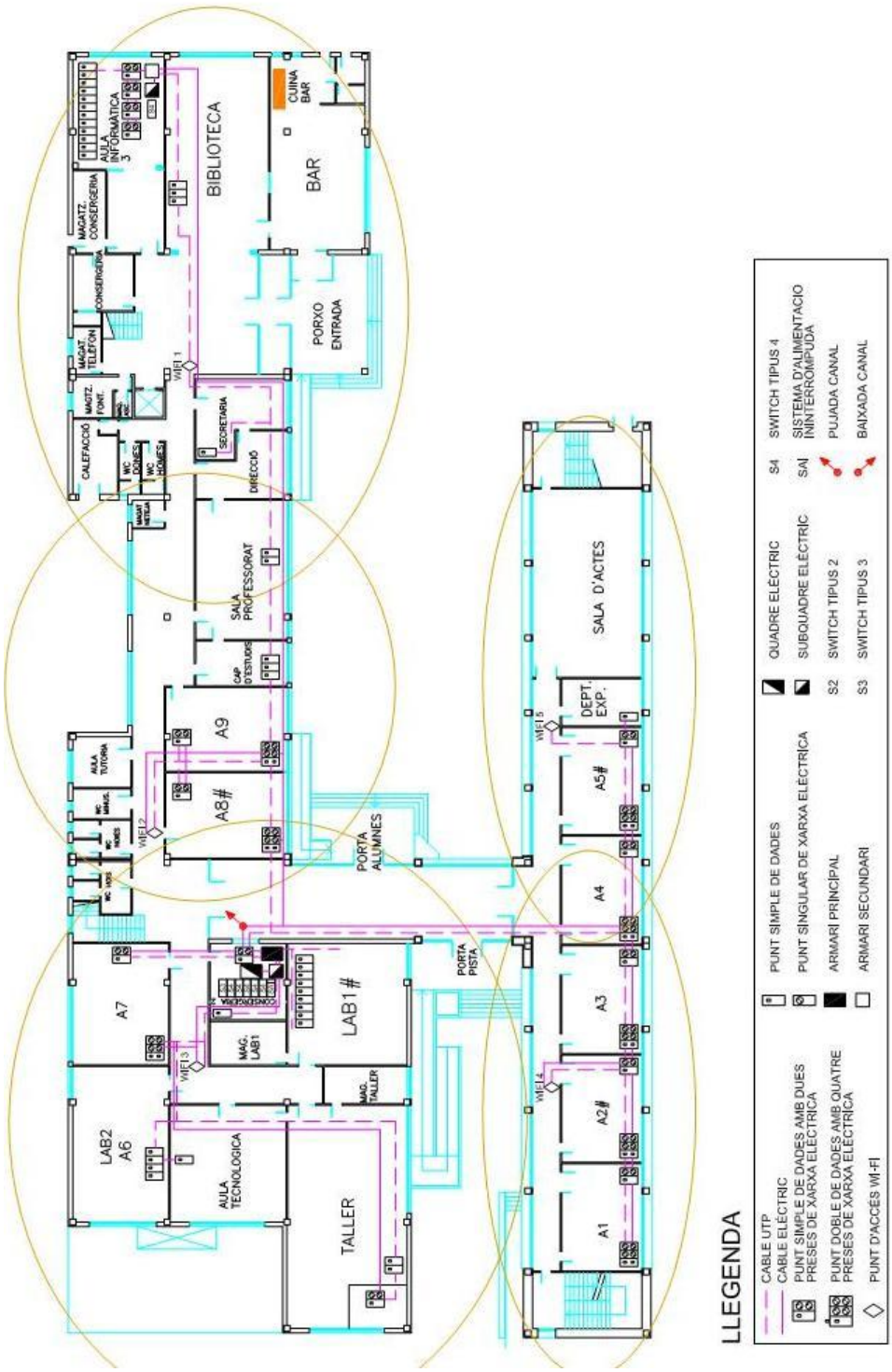



Figura 5.2: Plànol cablejat planta baixa.

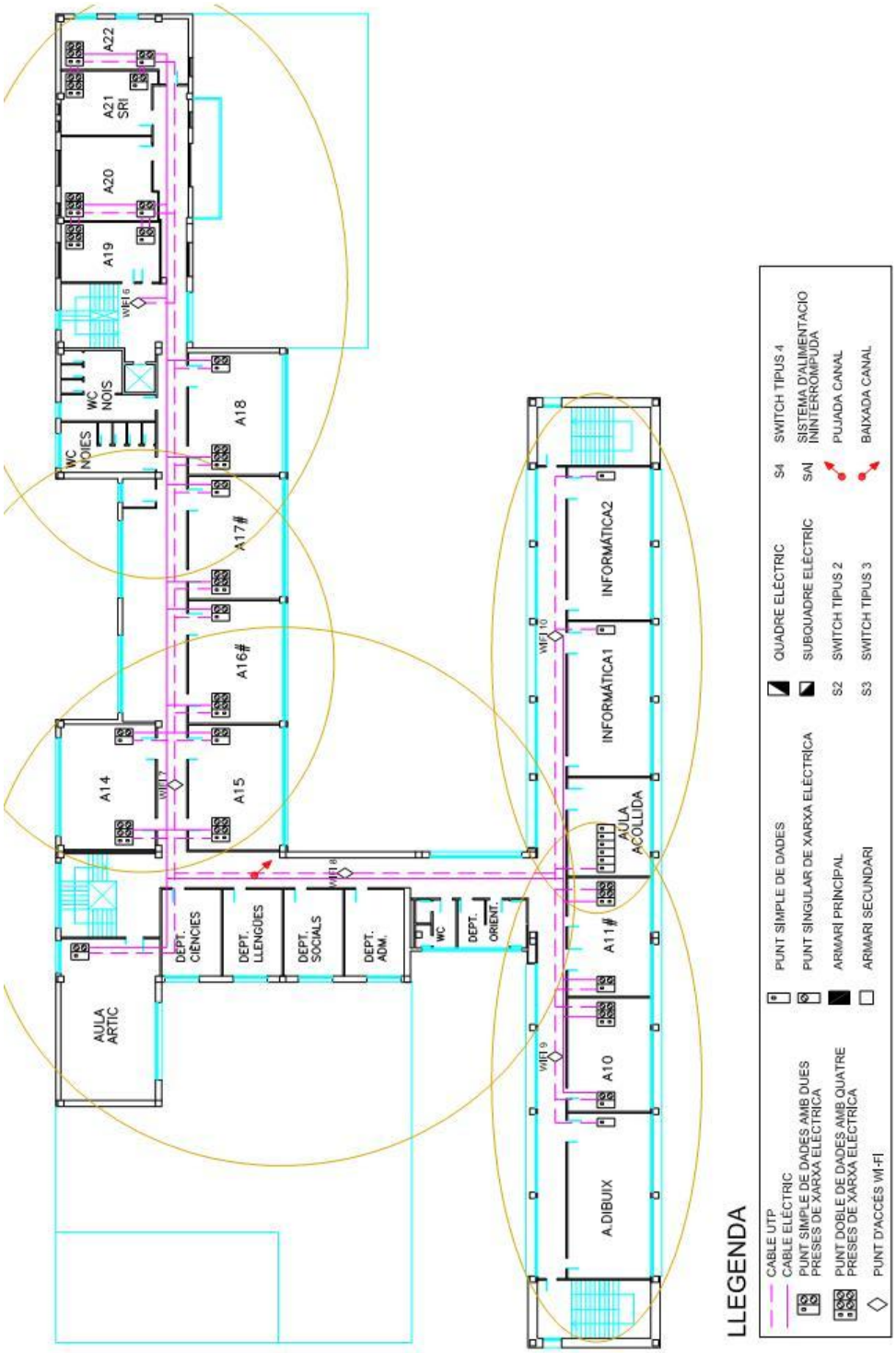



Figura 5.3: Plànol cablejat planta primera.

### 5.1.2 Separació de xarxes

Per realitzar una correcta divisió de la xarxa es classificaran els punts de xarxa i els equips en funció de les tasques que s'hagin de dur a terme en ells, del tipus d'usuaris que utilitzaran la xarxa i dels serveis que requereixin.

Seguint aquesta divisió es poden distingir fins a cinc tipus d'usuaris diferents:

1. Alumnat : Correspon als alumnes matriculats al centre. Realitzen activitats dirigides i treballs de classe. Aquesta xarxa haurà de tenir connexió a Internet , servei d'autenticació centralitzada i servei de dades centralitzat. Compren els punts de xarxa situats principalment a les aules i biblioteca.

2. Professorat : Correspon a professorat del centre. Realitzen activitats variades. Cal dotar-los de serveis d'autenticació centralitzada, servei de dades centralitzats i connexió a Internet. Compren els punts de xarxa situats a les sales de professors i als departaments corresponents. (opcional punts d'aules destinats als professors)

3. Direcció i PAS : Correspon a persones que realitzen tasques de direcció i administració del centre. Donat que les tasques administratives es troben centralitzades en Internet mitjançant l'aplicació SAGA, només serà necessari donar connectivitat a Internet. Compren els punts de xarxa situats als despatxos de secretariat, cap d'estudis, direcció i secretaria.

4. Professorat WI-FI : Es una xarxa sense fils per al professorat del centre. Seran aplicades les mateixes consideracions que a la xarxa de professorat.

5. Professorat extern WI-FI (eduroam) : Es una xarxa sense fils per a personal del Departament d'Educació aliè al centre. L'accés a aquesta xarxa es gestionat pel Departament. Només donarà accés a Internet.

Caldrà a més tenir algunes xarxes addicionals per facilitar la gestió dels equipaments de xarxa i per a la separació de servidors i xarxa externa.

Aquestes son :

1. Xarxa gestió d'equips : Permet gestionar remotament l'equipament de xarxa.

2. Xarxa servidors : Permet separar alguns dels servidors de la resta de la xarxa i afegir una protecció addicional a aquestos.

3. Xarxa externa : Permet connectar a Internet i connectar servidors que hagin de donar serveis al exterior (pàgina web de l'escola, etc.)

### 5.1.3 Adreçament IP.

Un cop separades les xarxes a nivell 2 (Ethernet) cal establir l'adreçament IP de cadascuna d'elles per poder encaminar paquets entre elles si s'escau.

L'adreçament IP de les xarxes serà el següent :

1. Xarxa Alumnes : La xarxa d'alumnes es la que més equips té de totes, així que per a aquesta xarxa es mantindrà l'adreçament actual del centre. La raó de fer això és haver de canviar la IP a la menor quantitat de estacions possibles. Es canviarà però la màscara de subxarxa, ja que la actual de 24 bits només permet 254 equips, se li configurarà una nova màscara de 16 bits per cobrir futures ampliacions del nombre d'equips. Els paràmetres IP d'aquesta xarxa son :

   - Adreçament : 192.168.0.0/16
   - Servidor xarxa alumnes : 192.168.0.100
   - Gateway per defecte : 192.168.0.1
   - Nombre màxim d'equips : 65536-3 (broadcast, xarxa i gateway) = 65533 equips. Aquest nombre d'equips és el mateix per les altres xarxes.

2. Xarxa Professors :

   - Adreçament : 10.1.0.0/16
   - Servidor xarxa Professors : 10.1.0.100
   - Gateway per defecte : 10.1.0.1

3. Xarxa Direcció i PAS

   - Adreçament : 10.2.0.0/16
   - Gateway per defecte : 10.2.0.1

4. Xarxa Docent WIFI :

   - Adreçament : 10.3.0.0/16
   - Gateway per defecte : 10.3.0.1

5. Xarxa Eduroam
    - Adreçament : 10.4.0.0/16
    - Gateway per defecte : 10.4.0.1
6. Xarxa Servidors
    - Adreçament : 10.5.0.0/16
    - Servidor central : 10.5.0.100
    - Gateway per defecte : 10.5.0.1
7. Xarxa Gestió d'Equips
    - Adreçament : 10.6.0.0
    - Gateway per defecte : 10.6.0.1
8. Xarxa Externa
    - Adreçament : 10.7.0.0/16
    - Gateway per defecte : 10.7.0.1

Amb aquestes modificacions s'ha previst i cobert futures ampliacions del nombre d'equips donant rangs IP i màscares de forma que el nombre d'equips possible sigui molt més gran que el nombre d'equips que s'espera tenir en un futur. Totes les adreces utilitzades son adreces reservades a ús privat.

### 5.1.4 ACLs i classificació del tràfic.

Quan ja s'han establert els adreçaments IP de cada xarxa cal establir quines connectivitats entre elles són necessàries i quines no són desitjades. Es seguiran les següents consideracions :

1. Xarxa Alumnes : Aquesta xarxa ha d'estar limitada a accedir a Internet. No ha de poder connectar a cap altra xarxa del centre. L'únic equip de la xarxa amb permís per accedir a la xarxa de servidors es el servidor de la xarxa d'alumnes.
2. Xarxa Professors : Aquesta xarxa ha d'estar limitada a accedir a Internet. No ha de poder connectar a cap altra xarxa del centre. L'únic equip de la xarxa amb permís per accedir a la xarxa de servidors es el servidor de la xarxa de professors..

3. Xarxa Direcció i PAS : Només ha de tenir accés a Internet.

4. Xarxa Docent WIFI : Ha de tenir accés a Internet i accés al servidor de professors.

5. Xarxa Eduroam : Només ha de tenir accés a Internet.

6. Xarxa Servidors : El servidor LDAP central que hi ha en aquesta xarxa només es accessible pels dos servidors ( el d'alumnes i el de professors). Ha de poder connectar també a Internet per la descàrrega d'actualitzacions.

7. Xarxa Gestió d'Equips : No te connectivitat amb cap altra xarxa i té connectivitat limitada amb Internet.

8. Xarxa Externa : Te connectivitat amb totes les xarxes.

Hi ha dos casos especials : Els servidors de professors i d'alumnes que han de poder connectar al servidor central. Més endavant en la secció de serveis de xarxa es mostraran els detalls de configuració dels servidors, lesconsideracions de seguretat i la forma en que es connecten.

La taula 5.1 mostra les connectivitats necessàries i prohibides entre les xarxes definides. Es fan servir 3 casos diferents, són els següents:

- SI : Vol dir que les xarxes tenen accés sense restriccions entre elles. En cas que una de les parts sigui un equip i no una xarxa vol dir que la xarxa té accés a un equip en concret.

- NO : Vol dir que es descarten els paquets.

- A NIVELL 2 : Vol dir que els equips estan a la mateixa xarxa.

| | IP Origen | Xarxa Alumnes | Xarxa Profes | WIFI Docent | Eduroam | Gestio | Servidors | Externa | Server Profes | Server Alumnes | PAS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| IP Destí | | | | | | | | | | | |
| Xarxa Alumnes | | | NO | NO | NO | NO | NO | SI | NO | A NIVELL 2 | NO |
| Xarxa Profes | | NO | | NO | NO | NO | NO | SI | A NIVELL 2 | NO | NO |
| WIFI Docent | | NO | NO | | NO | NO | NO | SI | SI | NO | NO |
| Eduroam | | NO | NO | NO | | NO | NO | SI | NO | NO | NO |
| Gestio | | NO | NO | NO | NO | | NO | SI | NO | NO | NO |
| Servidors | | NO | NO | NO | NO | NO | | SI | SI | SI | NO |
| Externa | | SI | SI | SI | SI | SI | SI | | SI | SI | SI |
| Server Profes | | NO | A NIVELL 2 | SI | NO | NO | SI | SI | | NO | NO |
| Server Alumnes | | A NIVELL 2 | NO | NO | NO | NO | SI | SI | NO | | NO |
| PAS | | NO | NO | NO | NO | NO | NO | SI | NO | NO | |

Taula 5.1: Taula de control d'accés IP

#### 5.1.4.1 Complement WIFI.

En el complement de xarxa sense fils es procurarà mantenir la configuració nova tant semblant a la actual com sigui possible.

Es definiran 2 xarxes sense fils mitjançant la configuració de 2 SSID (*Service Set Identifier*), el primer d'ells el SSID "docent" amb seguretat WPA-PSK (*Wireless Protected Acces - Pre Shared Key*), es a dir s'establirà una clau ja definida per connectar a la xarxa. Aquesta clau serà compartida per tothom que es connecti a la xarxa. Encara que aquesta sol·lució no és la mes segura, al menys no obliga a mantenir un servidor RADIUS operatiu al centre. A més el maquinari disponible no suporta la validació amb més d'un servidor RADIUS (*Remote Authentication Dial In User Service*) encara que es facin servir múltiples SSIDs.

L'altre SSID que es definirà serà "eduroam", aquest farà servir validació WPA-EAP, es a dir farà servir un servidor extern per validar els usuaris. Aquest servidor RADIUS extern es mantingut pel Departament d'Educació i el seu manteniment no suposa cap càrrega de treball per al centre.

### 5.1.5 Estructura lògica de la xarxa

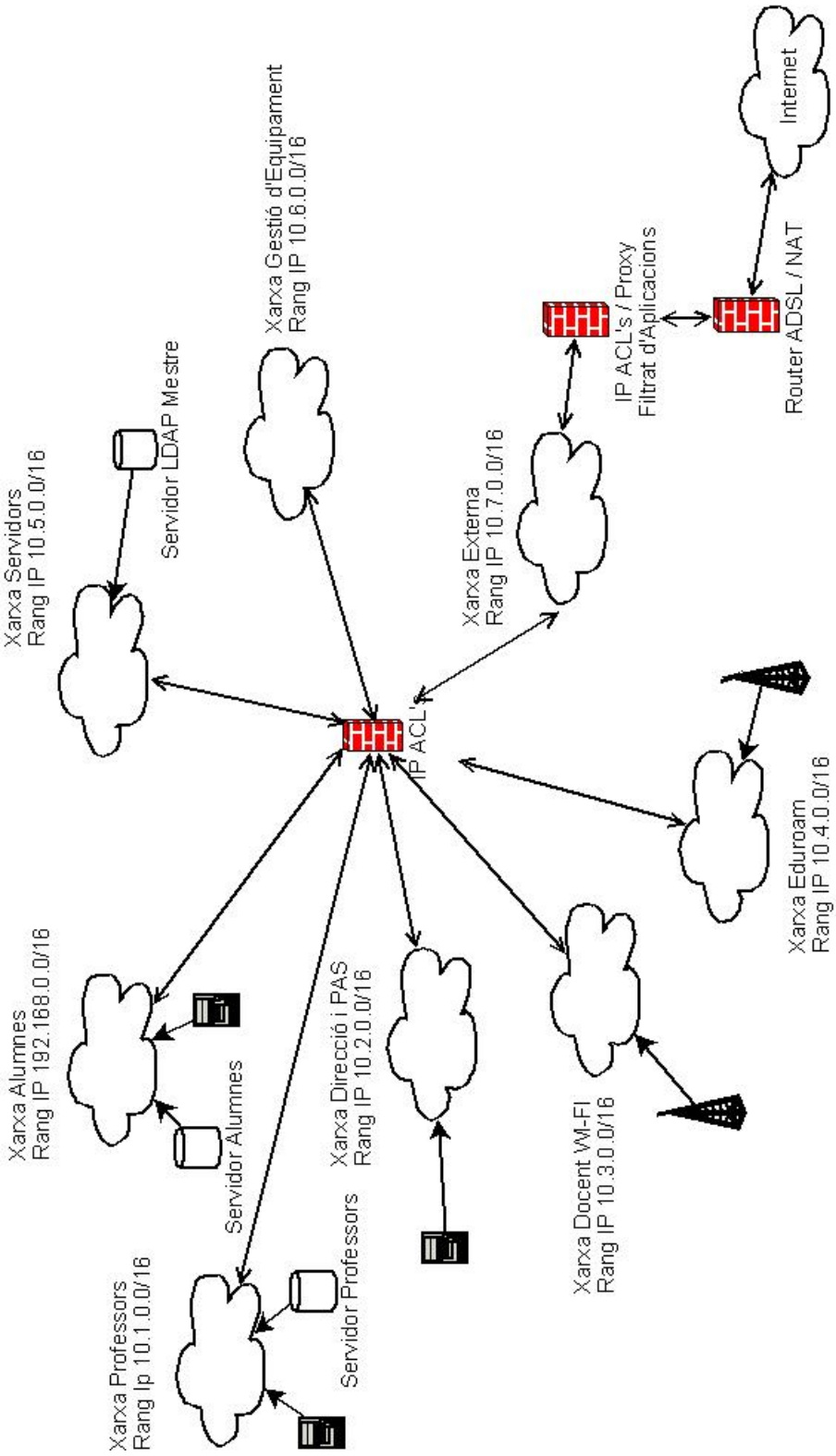



Figura 5.4: Estructura lògica de la xarxa.

A la figura 5.4 es pot veure un esquema lògic de la xarxa a implementar. Com es pot observar s'ha dividit la xarxa en diverses xarxes en funció dels usuaris i de l'ús que es fa de la xarxa. El tràfic a més es controlat per evitar connectivitats no desitjades entre les xarxes.

## 5.2 Serveis de xarxa

Un cop s'ha definit correctament la estructura de la xarxa conforme als requeriments esmentats amb anterioritat, cal especificar i dissenyar els serveis que seran necessaris per a obtenir un sistema informàtic que doni una funcionalitat real i útil.

Per raons de cost de flexibilitat i de no dependència dels fabricants el programari que es farà servir serà de lliure distribució. Es farà servir la distribució GNU/Linux Ubuntu server 7.10 com a plataforma sobre la qual s'implementaran els serveis.

Aquesta distribució és una distribució optimitzada per a funcions de servidor, té molt bon suport tant comercial com de la comunitat.

D'aquí en endavant es tractarà de decidir quines tecnologies i quin programari serà necessari per a complir els objectius proposats.

### 5.2.1 Validació d'usuaris

Abans de passar a considerar de quina manera es farà la validació d'usuaris es veuran alguns dels sistemes de validació d'usuaris existents per als servidors Linux . Els principals per a entorns productius són :

1. Fitxers locals : Aquest és el tipus més bàsic d'autenticació d'usuaris. Es basa simplement en arxius de text pla. El principal avantatge d'aquest sistema es la seva senzillesa. Per contra no permet la exportació a altres màquines si no és copiant els arxius i no està pensat per fer-ho servir com a base de dades centralitzada en una xarxa. Es desestima el seu us.

2. NIS (*Network Information Service*) : És us sistema d'autenticació centralitzat creat per SUN Microsystems. Té una arquitectura client-servidor en la qual els clients obtenen còpies dels arxius d'usuaris, de grups, noms de màquina, etc. Està basat en RPC (*Remote Procedure Call*) que és un protocol que permet que un programa faci crides a funcions que corren en una altra màquina. El mètode d'autenticació per a

la versió Linux de NIS suporta autenticació AUTH_UNIX, en la qual la crida s'identifica mitjançant el UID i GID de l'usuari Unix. Aquesta implementació té greus fallides de seguretat, ja que no implementa cap mecanisme criptogràfic. A més permet a qualsevol client NIS descarregar una còpia de la base de dades d'usuaris per dur a terme atacs fora de línia. Per aquestos motius es necessari decantar-se per tecnologies més modernes que ofereixin més flexibilitat i seguretat. Avui en dia NIS s'està veient desplaçat per LDAP (*Lightweigh Directory Acces Protocol*).

3. LDAP : És un protocol d'aplicació que permet l'accés a un servei de directori ordenat i distribuït. Les característiques d'aquest protocol es descriuen a 5.2.1.1 .

4. SAMBA : És la implementació d'una sèrie de protocols basats en NetBIOS originalment desenvolupats per Microsoft, Intel i 3Com. Les característiques d'aquest protocol es descriuen a 5.2.1.3

#### 5.2.1.1 LDAP

Per ser d'especial interès s'amplia la informació sobre LDAP.

El protocol LDAP té una arquitectura client-servidor. Un client LDAP pot connectar al port del servidor LDAP i demanar alguna de les següents operacions:

1. BIND : Autenticar-se i especificar una versió de LDAP.
2. Start TLS : Usar la extensió TLS (*Transport Layer Security*) de LDAPv3 per xifrar la connexió amb el servidor.
3. SEARCH : Buscar per obtenir un atribut donat.
4. COMPARE : Comprovar si una entrada conté un atribut donat.
5. Afegir entrades.
6. Esborrar entrades.
7. Modificar entrades.
8. Modificar DN : Moure o renombrar una entrada.
9. ABANDON : Avortar una petició prèvia.
10. UNBIND : Tancar connexió.

11. EXTENDED OPERATION : Altres operacions.

El directori LDAP té una estructura en arbre en la qual cada entrada té un únic DN (*Distinguished Name*) i un conjunt d'atributs. El DN es forma mitjançant la concatenació dels DN relatius de les entrades pare. Veure figura 5.5

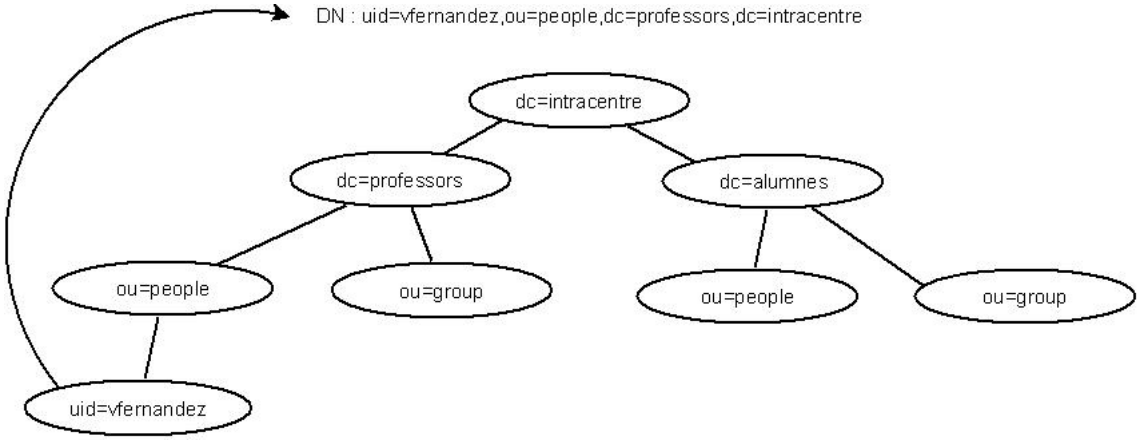



Figura 5.5: DN de les entrades.

LDAP també fa servir una base de dades de tipus BDB (*Berkeley Database*) que fa ús intensiu de l'indexat i caches de RAM. Així doncs si volem obtenir les dades d'un DN en particular LDAP buscarà en el arbre el identificador de la entrada i la base de dades BDB farà servir aquest per retornar la informació. Com es pot observar tant la cerca en arbres com el indexat de les entrades BDB proporcionen mètodes de consulta molt ràpida. Aquest és un dels punts forts de LDAP, la rapidesa de les consultes.

La versió a utilitzar de LDAP (OpenLDAP) es capaç de xifrar les connexions mitjançant TLS, el qual fa servir certificats x.509 per dotar a les transaccions de LDAP de integritat i confidencialitat.

A més LDAP proporciona un fi control mitjançant llistes de control d'accés per controlar la validació d'usuaris i quina informació podrà obtenir cada usuari. Es pot configurar que es demani autenticació abans d'accedir a les dades.

L'arbre LDAP es pot replicar en diversos servidors per aconseguir balanceig de càrrega i alta disponibilitat.

Per totes aquestes raons es farà servir LDAP per l'accés a la base de dades d'usuaris, grups i equips.

LDAP però per si sol és vulnerable a atacs que interceptin o capturin les dades que viatgen per la xarxa. Com es vol tenir un sistema resistent a

aquestos atacs s'utilitzarà TLS per xifrar les connexions a LDAP que hagin de viatjar per la xarxa.

#### 5.2.1.2 TLS

El principal objectiu del protocol TLS es proporcionar privacitat i integritat de dades entre dues aplicacions que es comuniquen. Actua entre la capa de transport TCP i la capa d'aplicació. Consta de dues parts diferenciades, el TLS Record Protocol i el TLS Handshake Protocol. El primer d'ells es fa servir per xifrar la connexió en una sessió TLS, el segon es fa servir per validar els equips i per l'intercanvi de claus de xifrat.

El TLS Record Protocol té dues propietats bàsiques :

1. La connexió és privada : Empra criptografia simètrica per al xifrat de les dades. Les claus utilitzades son aleatòries i negociades en cada sessió. Aquestes son negociades pel TLS Handshake Protocol. Admet un àmplia varietat d'algoritmes simètrics, en aquest treball s'empra AES 256 bits .

2. Proporciona integritat a la connexió : Les dades transmeses són verificades mitjançant funcions de hash segures (com MD5, SHA, etc) les quals permeten assegurar la integritat del missatge. En aquest treball s'empra SHA-160.

El TLS handshake protocol té tres propietats bàsiques :

1. La identitat de l'equip remot pot ser autentificada mitjançant criptografia asimètrica o de clau pública. En aquest treball s'empra RSA 1024 bits. Encara que segons Adi Shamir i Eran Tromer es possible trencar les claus RSA 1024, per a aquesta tasca es requeriria un any sencer de procés i la inversió de uns 10 milions de dolars. Amb hardware de propòsit general l'atac es impracticable a dia d'avui, així que en la pràctica és segur per al propòsit destinat i el funcionament serà més ràpid que implementant claus més grans.

2. La negociació de les claus de sessió és segura. Aquestes claus s'escullen aleatòriament, són generades a cada sessió i s'intercanvien xifrades mitjançant criptografia de clau pública. Veure figura 5.6.

3. La negociació és confiable : Un atacant no pot alterar les dades transmeses sense ser detectat.

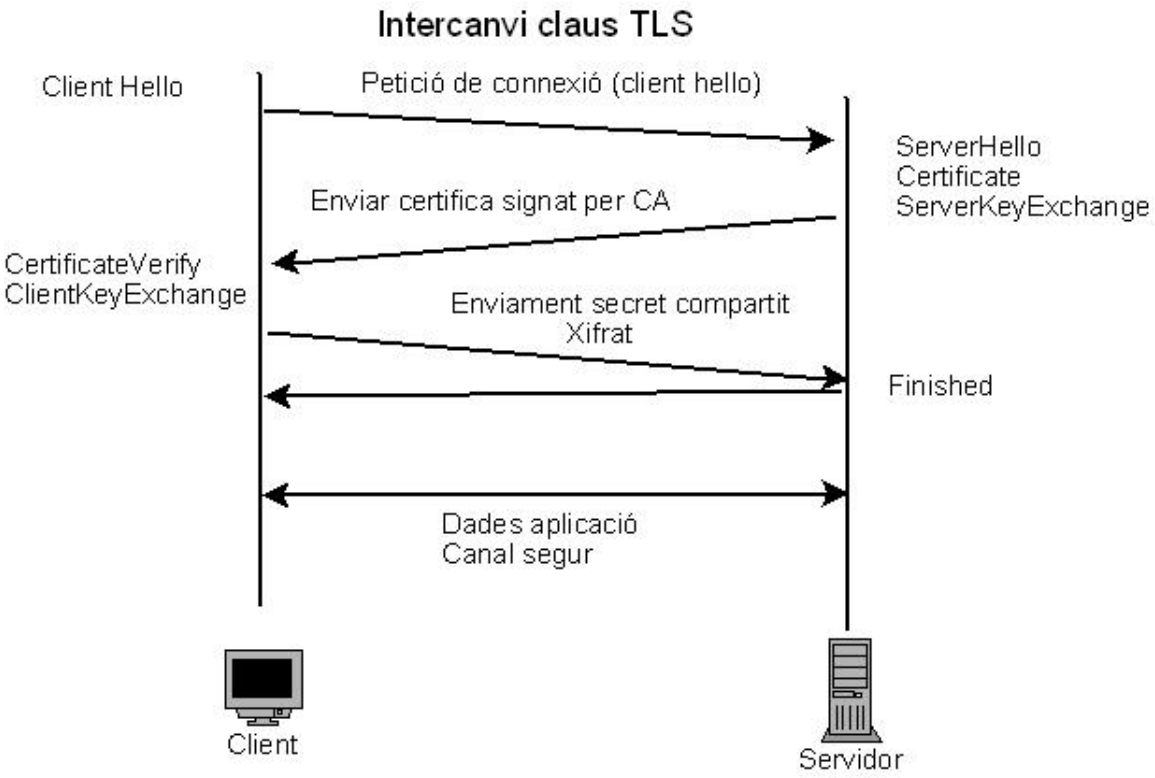



Figura 5.6: Intercanvi claus TLS

El punt més feble del sistema LDAP/TLS és que si es compromet el servidor és possible obtenir el parell clau privada/publica , desxifrar els missatges obtinguts de la xarxa mitjançant aquesta i obtenir les claus d'usuari. També seria possible obtenir la base de dades LDAP per dur a terme atacs fora de línia o alterar aquesta. Per evitar en la mesura del possible això els servidors només correran els serveis de xarxa totalment imprescindibles per dur a terme la seva tasca, no es podran obrir sessions remotes en aquestos i es configuraran els permisos dels administradors de LDAP per a que si es compromet algun dels servidors secundaris (els directament accessibles des de la xarxa) no s'obtingui informació suficient per obtenir informació dels altres servidors. El servidor mestre només és accessible pels servidors secundaris i a més aquestos tenen certificats signats per una CA (*Certificate Authority*) de forma que per connectar al màster en l'únic port obert (636 ldapssl) cal posseir un certificat vàlid.

A la figura 5.7 es pot veure el procés de signatura digital. Aquest tipus de signatura es basa en funcions resum o funcions hash. Per a aquest projecte es fa servir SHA com a funció de resum. Aquesta crea un resum de 160 bits

a partir de dades que poden ésser molt més grans. D'aquesta manera per signar el certificat es procedeix a calcular el hash SHA del certificat, un cop calculat es xifra el resum amb la clau privada que correspon a la clau publica continguda al certificat, i després es torna a xifrar amb la clau privada de l'entitat certificadora CA. Per verificar el certificat es procedeix a desxifrar el hash primer amb la clau pública de la CA, després amb la clau publica continguda al certificat. Un cop es té el hash en clar es calcula el hash del certificat i es comparen. Si coincideixen és per que el hash del certificat ha estat xifrat per informació que només té qui ens ho ha enviat i que esta xifrat també per una entitat en la que es confia (CA).D'aquesta manera si es confia en qui ha signat el missatge, es confia que la clau publica que s'ha rebut pertany a qui ha de pertànyer. D'aquesta manera s'eviten atacs de suplantació del servidor, ja que un agressor no pot signar un certificat amb una clau privada que no posseeix (la de la CA) i per aquesta raó ni clients ni servidors basats en TLS confiaran en ell i se li denegarà la connexió.

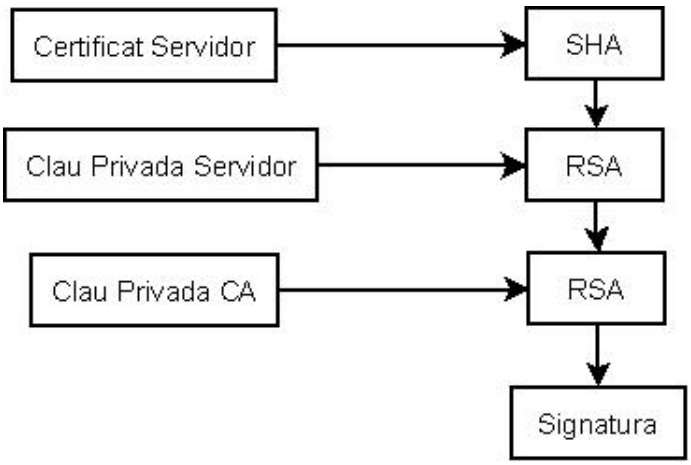



Figura 5.7: Model teòric de signatura digital.

A la figura 5.8 es pot veure el procés de verificació de signatura digital.

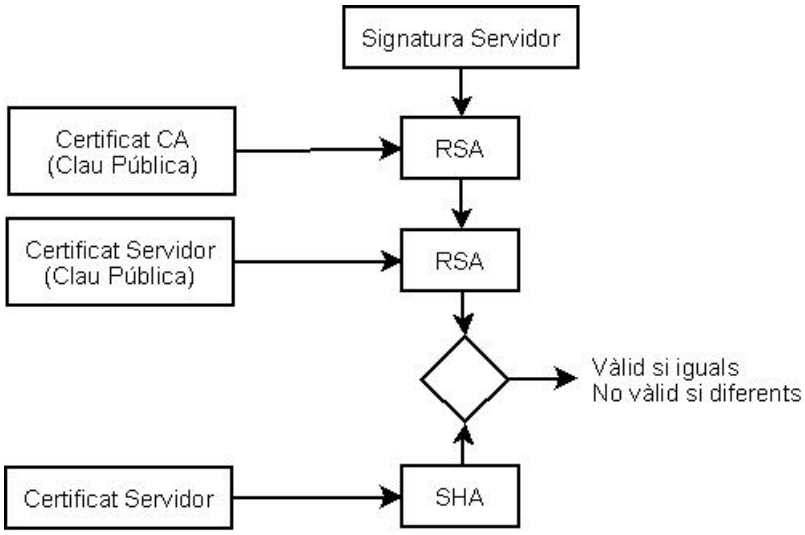



Figura 5.8: Verificació signatura digital.

#### 5.2.1.3 SAMBA

Els protocols anomenats SMB (*Server Message Block*) i més recentment CIFS (*Common Internet File System*) són una família de protocols clients-servidor que permeten , entre altres funcions, la validació centralitzada d'usuaris i l'exportació de sistemes d'arxius a través de xarxa. Aquestos protocols han esdevingut ,degut a la posició massivament dominant de Microsoft en el mercat dels ordinadors personals, un estàndard "de facto" i són necessaris a l'hora de implementar serveis de autenticació d'usuaris i equips, compartició d'arxius per xarxa i resolució de noms en entorns MS Windows. Per sort l'equip de desenvolupament del Samba Project ha implementat gran part d'aquestos protocols i SAMBA 3 ja és capaç de suportar autenticació segura mitjançant NT Lan Manager v 2, com també d'obtenir les dades relatives als usuaris i els equips client de directoris LDAP. L'arquitectura dels protocols esmentats és també una arquitectura client-servidor.

Per ser d'especial interès la seguretat en aquest treball es detallarà a continuació el funcionament de NT Lan Manager v2 pel que fa a l'autenticació.

L'esquema d'autenticació NTLMv2 és un esquema del tipus desafiament-resposta. L'autenticació d'aquest tipus es basa en un esquema de secret compartit. Es a dir el servidor té una còpia de la contrasenya o de un derivat fix d'aquesta, en aquest cas el hash MD4 de la contrasenya, de cada estació i de cada usuari.

Quan un usuari vol autentificar-se l'estació client envia la petició al servidor, el servidor genera llavors un desafiament aleatori i l'envia al client. En

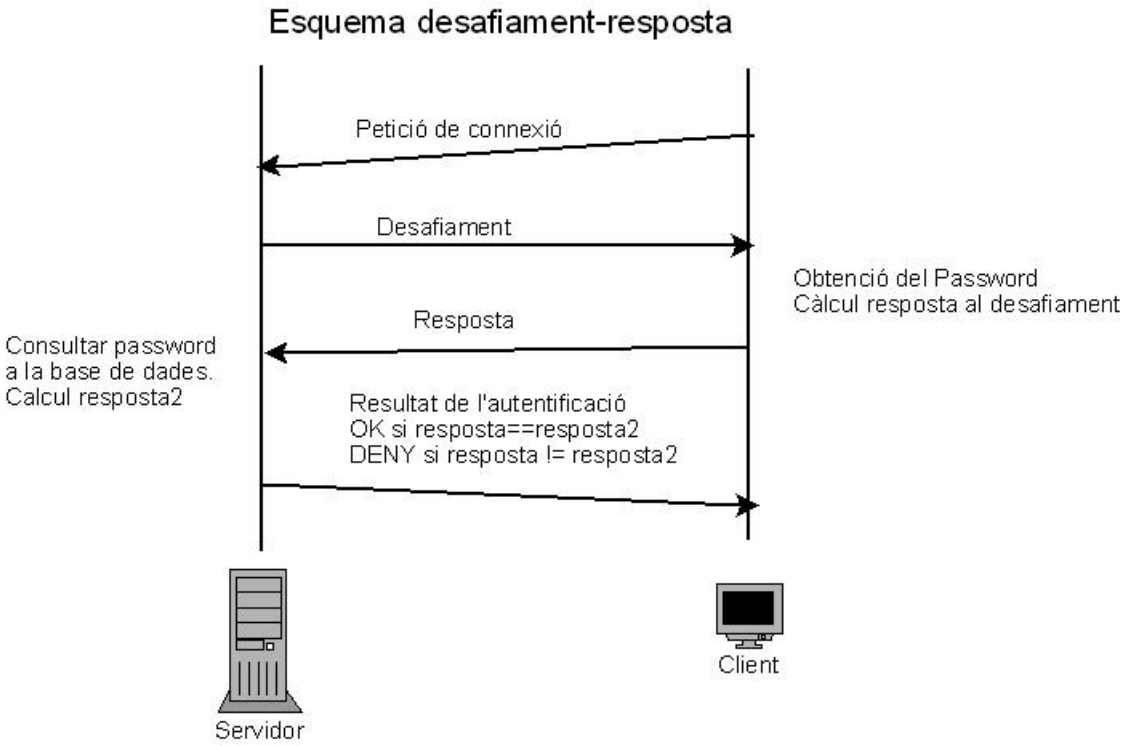



Figura 5.9: Esquema autenticació Desafiament-Resposta

aquest punt el client fa servir la contrasenya que se li ha entrat per calcular mitjançant funcions criptogràfiques una resposta que és enviada al servidor. Quan el servidor rep la resposta fa el mateix càlcul que ha fet el client fent servir la còpia de la contrasenya que té emmagatzemada i compara el resultat amb la resposta del client. Si la comparació és positiva dona accés al client, si no ho és el refusa.

La autenticació de les màquines client funciona de manera similar, l'únic que canvia és que la contrasenya d'estació no l'entra l'usuari sinó que ha estat negociada i s'ha intercanviat prèviament en el procés d'addició de la màquina al domini.

Per evitar que la negociació de la clau de la màquina pugui ésser interceptada la clau es xifra amb la contrasenya de l'administrador (requerida per introduir màquines al domini) abans de ser enviada.

Per al càlcul de la resposta al desafiament en NT Lan Manager v2 es fa servir l'algoritme de la figura 5.10.

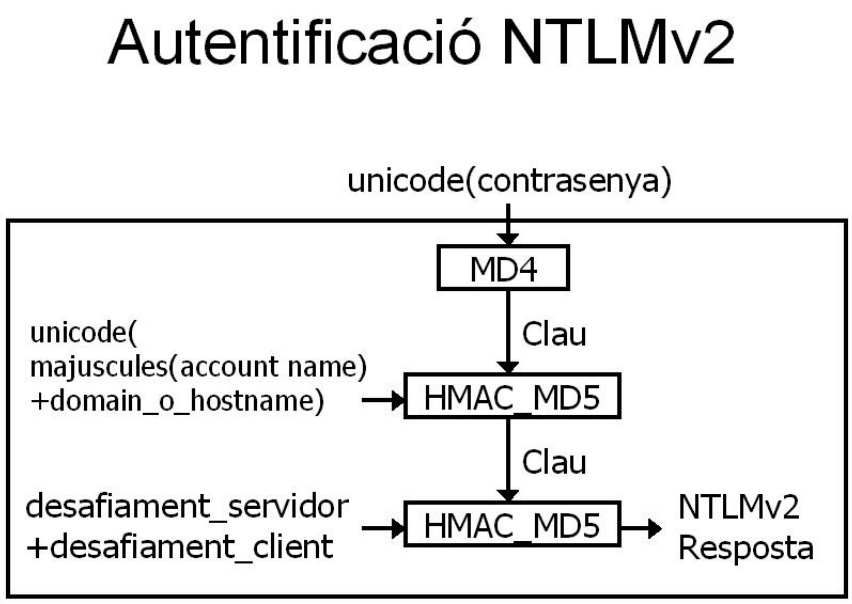



Figura 5.10: Càlcul resposta NT Lan Manager v2

El mètode HMAC-MD5 [HMAC] es basa en la següent operació :

1. Primerament és necessari disposar d'una funció de hash robusta, en el nostre cas MD5.

2. Es defineix B com el nombre d'octets de les dades. (mida del desafiament)

3. Es defineix K com la clau de xifrat (pot ser tan gran com B).

4. Es defineix ipad = 0x36 repetit B vegades.

5. Es defineix opad = 0x5c repetit B vegades.

Sabent això es calcula la funció HMAC-MD5 com : MD5(K xor opad, MD5(K xor ipad, dades))

Com es pot veure a la taula 5.2, la fortalesa de NTLMv2 és de l'ordre de 128 bit. Això fa que en la pràctica un atac de força bruta sigui impracticable.

| Hash de la contrasenya | MD4 |
|---|---|
| Longitud hash contrasenya | 128 bit |
| Longitud clau Desafiament / Resposta | 128 bit |
| Algoritme Desafiament / Resposta | HMAC_MD5 |
| Longitud Desafiament / Resposta | 128 bit |

Taula 5.2: Fortalesa de la autenticació NTLMv2

El punt més feble del sistema és que al contrari que els passwords de Unix/Linux la informació dels hash de 128 bit utilitzats per a fer els còmputs de les respostes als desafiaments es guarda en clar al servidor, ja que en cas contrari no podria fer els càlculs pertinents per la validació. Així doncs si s'aconsegueix obtenir la base de dades on es guarden seria possible calcular fàcilment les respostes als desafiaments del servidor i obtenir accés no autoritzat. El sistema de permisos de LDAP i el fet que només l'usuari *root* tingui accés als arxius on es guarden les credencials de connexió al LDAP fa que sigui necessari comprometre el servidor per obtenir el llistat d'aquesta informació.

Un altre punt feble comú a tots i cada un dels sistemes d'autenticació basats en contrasenya és la elecció de contrasenyes febles, basades en diccionari o fàcilment esbrinables. Un atac a una contrasenya feble és molt més viable que intentar trencar LDAP/TLS o SAMBA/NTLMv2 per força bruta.

#### 5.2.1.4 Equips client.

És necessari pensar també quins equips clients es tindran a la xarxa i quina és la millor manera de validar usuaris en aquestos.

Els equips clients que es poden trobar als centres d'educació secundaria són bàsicament de tres tipus :

- Clients Windows XP : Els clients d'aquest tipus permeten nativament l'autenticació centralitzada mitjançant dominis NT o Active Directory. La implementació de la part de servidor de dominis NT està lliurement disponible en el paquet de programari lliure SAMBA 3.0 . La futura versió SAMBA 4.0 suportarà a més Active Directory ( LDAP + Kerberos) i introduirà millores en la seguretat, escalabilitat i flexibilitat de configuració. Desgraciadament la nova versió de SAMBA és en aquestos moments altament experimental i com s'està dissenyant un sistema que ha d'estar en un entorn productiu es desestima la seva utilització. La versió 3.0 de samba és capaç també de consultar les dades d'usuaris i equips en un directori LDAP. Es farà servir aquesta

característica per poder emmagatzemar totes les dades d'usuaris en un directori LDAP i es validaran els usuaris a les estacions windows XP mitjançant SAMBA.

- Plataformes MacOSX i GNU/Linux : Poden tenir diverses maneres d'autentificar els usuaris. Per raons de flexibilitat , seguretat i rendiment es farà servir LDAP per a l'autenticació de clients MacOSX i Linux.

### 5.2.2 Compartició de dades

Per decidir quin tipus de programari és necessari per a la compartició de dades també s'ha de veure de quins serveis de compartició de dades es disposa en Linux. Els principals per a entorns de producció són:

1. NFS : És un protocol originalment desenvolupat per Sun Microsystems, Inc., proporciona accés a arxius compartits a través de la xarxa. La utilització d'aquest protocol es desestima ja que no ofereix seguretat. Al igual que NIS només demana l'UID i GID de l'usuari que fa la petició i confia que l'usuari és qui diu ser.

2. SAMBA : Els protocols implementats en el paquet SAMBA permeten accedir a arxius compartits a través de la xarxa. La validació dels usuaris es fa amb l'anteriorment descrit NTLMv2. Per aquesta raó l'autenticació dels usuaris és robusta. I per aquesta raó es farà servir SAMBA per a la compartició d'arxius.

És procedirà novament a considerar quin tipus d'equips client disposarà a la xarxa. Aquest pas és necessari ja que cal considerar prèviament amb quin tipus d'aplicació és compatible cada client i després decidir com es farà l'intercanvi de dades.

1. Clients Windows XP : Permeten accedir a sistemes d'arxius per xarxa mitjançant protocols privatius basats en Netbios (SMB). Per sort el paquet de software SAMBA 3.0 implementa clients i servidors de lliure distribució d'aquestos serveis. Per aquest tipus de clients es farà servir doncs el seu sistema nadiu, a la part de servidor es farà servir SAMBA 3.0.

2. Clients MacOSX : Poden muntar sistemes d'arxius diversos, des de AFP (*Apple Filing Protocol*), NFS (*Network File System*), SMB, etc. Per a implementar AFP cal programari addicional en la part de servidor i

no ofereix millors prestacions que SMB , el sistema NFS es desestima per ser insegur (no implementa cap tipus de autenticació robusta ni criptografia). Així doncs es farà servir SAMBA com a client per a l'accés als arxius.

3. Clients GNU/Linux : Suporten una amplia varietat de protocols de compartició d'arxius. Per a aquest treball es farà servir SAMBA.

El punt més feble d'aquestos sistemes d'arxius per xarxa és que cap d'ells ofereix de forma nativa criptografia. Per aquesta raó les dades que viatgen a la xarxa podrien ser interceptades. La divisió de xarxes que s'ha fet prèviament impedeix que es pugui espiar tràfic d'altres xarxes i d'aquesta manera aquest problema queda delimitat a la xarxa on es troba l'agressor.

### 5.2.3 Serveis Proxy

El servei de Proxy HTTP té com a objectiu principal minimitzar al màxim el tràfic amb Internet. Es pot aconseguir reduir el tràfic a Internet mitjançant una memòria cache d'arxius que guarda i serveix localment els arxius consultats. En entorns com un centre educatiu és especialment útil ja que molts dels accessos són efectuats per un nombre important de clients sobre un mateix arxiu. És l'exemple clar de tota una classe de més de 20 equips accedint a la pàgina web que diu el professor. A més com hi han pàgines que son consultades molt sovint es poden arribar a grans percentatges de "cache hit", en algunes pàgines es poden assolir percentatges del 99% . També es fa cache de les actualitzacions de software (antivirus i altres). Tot plegat permet una dràstica reducció de l'ocupació de la connexió externa, millora en gran mesura la velocitat d'accés als continguts i proporciona una millor satisfacció a l'usuari final.

A la figura 5.11 es pot veure un esquema de funcionament del proxy.

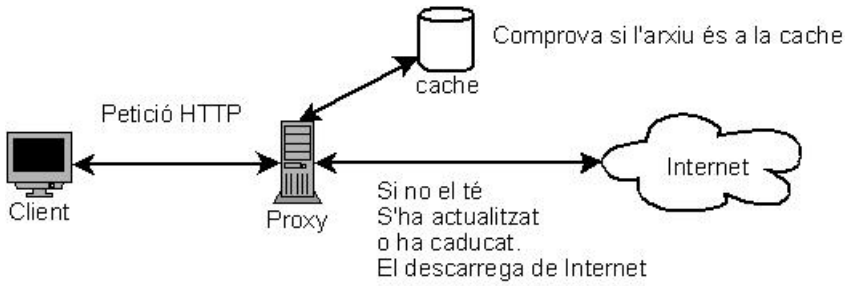



Figura 5.11: Esquema funcionament proxy HTTP.

### 5.2.4 Serveis Gestió continguts

Juntament amb el servei de proxy i funcionant en estreta col·laboració amb aquest es farà servir el programa de lliure distribució (GPL v2. per usos no comercials) DansGuardian. Aquest programari permet filtrar utilitzant diferents mètodes. Aquestos mètodes inclouen filtrat URL i dominis, filtrat de paraules clau, filtrat de tipus MIME, filtrat per extensió d'arxius, etc.

Encara que DansGuardian porta ja algunes configuracions per defecte tots els mètodes de filtrat poden ser configurats per adequar-se al tipus de contingut que es vol eliminar.

A més de filtrar continguts es possible filtrar els dominis als quals accedeixen a través del port 80 (TCP) aplicacions de missatgeria instantània de tipus messenger i similars.

Per aconseguir això últim cal parar atenció als registres que genera l'aplicació i denegar els dominis sospitosos. A més es clar s'ha de denegar les connexions a ports que no s'hagin de fer servir.

D'aquesta manera s'aconsegueix que les aplicacions de missatgeria instantània deixin de funcionar.

A la figura 5.12 es pot veure l'esquema de funcionament del gestor de continguts.

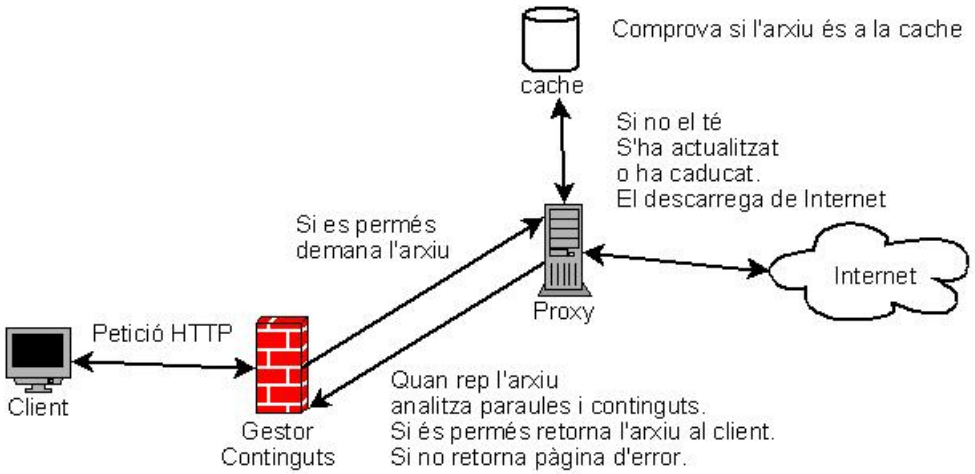



Figura 5.12: Esquema funcionament Gestor de Continguts.

### 5.2.5 Servei de filtrat d'aplicacions Peer to Peer.

Les aplicacions d'intercanvi d'arxius Peer to Peer (en endavant P2P) són freqüentment utilitzades per descarregar programes i materials audiovisuals. Aquestos materials freqüentment violen els drets dels legítims propietaris del

copyright, a més són una via poc controlable per la qual es podria accedir a continguts no desitjables i consumeixen un gran ample de banda de la connexió externa. Per aquestes raons és molt desitjable eliminar el tràfic P2Pa la xarxa.

Per reduir al mínim les possibilitats que aquestos programes donin problemes a la xarxa implementada es pot abordar la seva eliminació des de diversos fronts.

El primer consisteix en denegar el tràfic als ports utilitzats freqüentment per aquestes aplicacions, o millor encara, denegar el tràfic a tots els ports i permetre només aquells que siguin estrictament necessaris com el 80 (HTTP).

El problema és que alguns d'aquestos programes intenten connexions a través del port 80 i per aquesta raó cal fer servir programari capaç d'analitzar els paquets a nivell de la capa d'aplicació.

Es farà servir IPP2P, que és un programari que treballa en la capa d'aplicació i permet identificar quins paquets pertanyen a aplicacions P2P i eliminar-los selectivament.

En alguns entorns el filtre IPP2P pot donar falsos positius i bloquejar alguns serveis legítims de xarxa, això pot passar en rares ocasions. En el cas que passi alguna cosa així serà necessari estudiar quin servei o serveis no funcionen i prendre les mesures pertinents inclosa la desactivació del filtre si s'escau.

## 5.3 Necessitats d'administració

En aquest apartat es detallaran quines necessitats d'administració tindrà el sistema dissenyat. Aquestes s'han de mantenir al mínim possible per no fer el manteniment massa costós.

Les necessitats es divideixen en els següents tipus:

- Manteniment de maquinari i programari.
- Copies de seguretat.
- Comprovació dels registres.
- Altes i baixes d'usuaris.

### 5.3.1 Manteniment del maquinari i programari.

Aquest tipus de manteniment, que inclou les reparacions dels equips de xarxa i els ordinadors, la reinstal·lació de software tant de estacions de treball

com de servidors i la resolució d'incidències, és un servei que proporcionen empreses externes contractades pel Departament d'Ensenyament i no suposen costos addicionals pels centres. El centre només s'ha de preocupar de posar en coneixement de l'empresa adjudicatària les incidències que es produeixin.

### 5.3.2 Copies de seguretat.

És més que recomanable que es facin còpies periòdiques de les dades del servidor i al menys una còpia del sistema sencer, tant d'estacions de treball com del servidor, cada cop que aquestos s'actualitzen o es canvien configuracions.

Hi han diversos sistemes de còpia de seguretat, des de sistemes de cinta magnètica i suports òptics fins a servidors dedicats.

Un dels sistemes més pràctics i un dels més barats amb diferència consisteix en fer les còpies a un disc dur extern d'alta capacitat. Aquest sistema té múltiples avantatges, com és el seu baix cost, la alta capacitat d'emmagatzematge i la seva gran facilitat d'utilització.

Les còpies de seguretat poden ésser efectuades per personal del centre o per tècnics externs del servei preventiu insitu, aquestos pertanyen a empreses externes contractades pel Departament d'Ensenyament i tampoc suposen cost addicional per al centre.

### 5.3.3 Comprovació dels registres.

Els registres generats pel proxy i pel gestor de continguts donen informació precisa dels continguts accedits des de la xarxa. És recomana revisar-los periòdicament per permetre o denegar l'accés a dominis o pàgines en funció del seu contingut. És responsabilitat del centre decidir quins continguts han de ser accessibles i quins no. Aquesta tasca és recomanable que la dugui a terme personal del centre.

### 5.3.4 Altes i baixes d'usuaris

És una tasca necessària encara que a vegades feixuga. És necessari donar d'alta els usuaris legítims del sistema i donar de baixa aquells que no s'hagin de tornar a connectar.

# Capítol 6

# Implementació final del sistema

En aquest apartat es detalla la configuració de tot l'equipament necessari per a la implantació del sistema. Per a la implementació s'ha de tenir en compte les restriccions i recomanacions que s'han definit al capítol anterior.

## 6.1 Estructura de la xarxa

### 6.1.1 Descripció dels protocols necessaris.

Al capítol anterior s'ha vist la part purament física de la xarxa. Ara és moment de veure quins protocols de xarxa es faran servir per a aconseguir configurar la xarxa tal i com a la figura 5.5.

Aquestos protocols són :

- 802.1q : Protocol que permet transmetre i rebre paquets de varies LAN virtuals (VLAN) mitjançant un únic enllaç.
- STP (*Spanning Tree Protocol*) : Protocol que permet evitar bucles a la xarxa i configurar enllaços redundants.

#### 6.1.1.1 802.1q

És un protocol que opera en la capa 2 de l'arquitectura OSI. És fonamental en el disseny ja que només hi han dos enllaços entre armaris. Aquest protocol permet el pas de diferents VLAN pel mateix enllaç. Per a aconseguir això el protocol modifica la capçalera Ethernet inserint-hi un identificador de paquet que defineix a quina VLAN pertany.

A la figura 6.1 es mostra la modificació que fa el protocol.

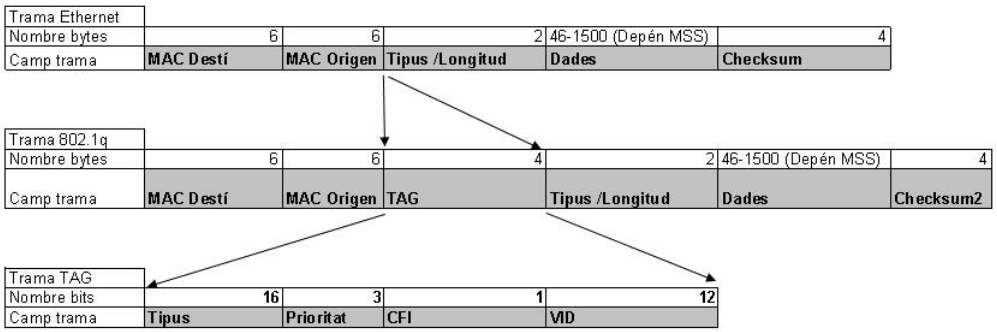



Figura 6.1: Trames protocol 802.1q [AXVLN]

El funcionament detallat del protocol es pot consultara la bibliografia [AXVLN].

#### 6.1.1.2 Spanning Tree Protocol (STP)

És un protocol de xarxa de la segona capa OSI, (nivell d'enllaç de dades). Està estandarditzat pel IEEE (IEEE_802.1D).

La seva funció és la de gestionar la presència de bucles en topologies de xarxa a causa de l'existència d'enllaços redundants (necessaris en molts casos per a garantir la disponibilitat de les connexions). El protocol permet als dispositius d'interconnexió activar o desactivar automàticament els enllaços, de manera que es garanteix que la topologia està lliure de llaços.

Quan hi ha llaços en la topologia de xarxa, els dispositius d'interconnexió de nivell d'enllaç re envien indefinidament les trames broadcast i multicast, al no existir cap camp TTL (*Time To Live*, Temps de Vida) en la Capa 2 (tal com ocorre en la Capa 3), aquestos paquets queden indefinidament a la xarxa. Es consumeix llavors una gran quantitat d'ample de banda, i en molts cas la xarxa queda inutilitzada.

La solució consisteix a permetre l'existència d'enllaços físics redundants, però creant una topologia lògica lliure de llaços.

STP crearà un arbre lògic de connectivitats entre els equips de xarxa permetent solament una trajectòria activa alhora entre dos dispositius de la xarxa (això prevé els bucles) però manté els camins redundants com reserva, per a activar-los en cas que el camí inicial falli.

Si la configuració de STP canvia, o si un segment en la xarxa redundant arriba a ser inassolible, l'algorisme reconfigura els enllaços i restableix la connectivitat activant un dels enllaços de reserva.

Existeixen diverses variants del Spaning Tree Protocol, degut principalment al temps que triga l'algorisme utilitzat a convergir. Una d'aquestes variants és el RSTP (*Rapid Spanning Tree Protocol*) que és la que implementa el nostre equipament.

Encara que es faci servir 802.1q i VLANs no es necessari activar ni configurar 802.1w MSTP (*Multiple Spanning Tree Protocol*) ja que l'equipament utilitzat bloqueja totes les VLAN quan bloqueja un port per acció del RSTP.

El funcionament detallat del protocol es pot consultara la bibliografia [AXSTP].

Per defecte RSTP estarà actiu a tots els ports dels switches.

### 6.1.2 Vlans necessàries.

1. VLAN Alumnes : Amb VID 2 correspon a la xarxa d'alumnes.
2. VLAN Professors : Amb VID 3 correspon a la xarxa de professors.
3. VLAN Direcció : Amb VID 4 correspon a la xarxa de direcció i PAS.
4. VLAN docent WIFI : Amb VID 5 correspon a la xarxa docent WIFI (WPA-PSK).
5. VLAN eduroam WIFI : Amb VID 6 correspon a la xarxa eduroam WIFI (WPA-EAP).
6. VLAN Servidors : Amb VID 7 correspon a la xarxa de servidors.
7. VLAN Gestió equips : Amb VID 8 correspon a la xarxa de gestió d'equipament.
8. VLAN externa : Amb VID 9 correspon a la xarxa de sortida a Internet.

### 6.1.3 Classificació dels punts de xarxa.

És necessari recórrer el centre amb el plànol d'instal·lació a la mà i apuntar en un paper l'etiqueta de cada punt i a quina xarxa haurà de pertànyer aquest.

Les recomanacions generals per a classificació són:

1. Biblioteca, aules en general, laboratoris i aules d'Informàtica : Els punts d'aquests espais es recomana posar-los a la xarxa d'alumnes.
2. Sales de professors, punts d'aules per a professors, departaments i despatxos del professorat : A la xarxa de professors.

3. Direcció i secretaria : A la xarxa de direcció i PAS.

4. Punts d'accés : És un cas especial, es configuraran aquests punts com "AP" al programa swgen. Aquest programa ha estat desenvolupat expressament per aquest treball i genera les configuracions dels switches a partir de la informació entrada per l'usuari. Els detalls es poden consultar a la secció 6.1.5.

5. Enllaços entre equips : És un cas especial, es configuraran aquests punts com "trunk" al programa swgen .

Per exemple si tenim un punt etiquetat com "R1SS3-18" i el volem posar a la xarxa de professors, ja que està a la sala de professors, cal apuntar-lo com "R1SS3-18 Xarxa professors".

### 6.1.4 Determinació de ports dels equips.

Un cop apuntada l'etiqueta de cada punt i la xarxa on ha de anar s'emprarà el següent procediment per determinar quina classe de punt és cada port de l'equip.

La descodificació de l'etiqueta de xarxa és :

- La "R" vol dir RACK i designa l'armari on és l'equip. Per exemple R2 voldria dir rack 2.

- "SS" vol dir switch secundari. Això designa un dels switches Zyxel ES2024. Per exemple SS3 designaria el tercer switch secundari començant per dalt que hi ha a l'armari designat per "R".

- -numero : El nombre designa el port de l'equip en qüestió.

Per exemple "R1SS3-18" vol dir el port 18 del tercer switch secundari de l'armari 1.

Un cop es sap a quina xarxa ha d'anar cada port de cada equip. Es procedeix a fer servir el programa swgen, desenvolupat per a aquest projecte.

### 6.1.5 Configuració switchs.

Per a generar l'arxiu de configuració de cada equip es farà servir el programa `swgen`. Aquest programa només demana de quin tipus és cada port del switch i alguna informació rellevant com la direcció IP de l'equip i el nom del centre.

Amb aquesta informació genera un arxiu de configuració que es podrà carregar a l'equip que s'hagi de configurar.

El programa fa servir el terme "boca" per referir-se a un port de l'equip, la idea de fer servir aquesta paraula és per fer més intuïtiva la configuració dels equips a usuaris poc experimentats.

Junt amb aquest treball es distribueix també un binari compilat per linux 64 bit i el codi font del programa.

#### 6.1.5.1 Detalls de funcionament programa swgen.

El programa swgen assigna a cada tipus de port una màscara en que cada valor pot ser :

- 0 : Aquest tipus de port no té accés a la Vlan.
- 1: Té accés a la VLAN
- 2:Té accés a la VLAN amb *tagging* 802.1q. (Es fa servir als punts d'accés 802.1q i per *trunking*).

Aquesta màscara es guarda en una matriu en la qual cada fila correspon a una interfície i cada columna correspon a l'accés que té en una determinada VLAN.

Com a l'arxiu de configuració se li ha de passar una llista de ports per a cada VLAN es llegeix la matriu per columnes i es generen 3 cadenes de text que corresponen a la llista de ports que cada VLAN tindrà com a permesos (1), permesos amb 8021q (2) i prohibits (0). Un cop fet això per a cada VLAN queden guardades una sèrie de cadenes. Aquestes contenen informació rellevant a la configuració.

El programa llavors llegeix l'arxiu que correspongui a la plantilla de cada model de switch i substitueix els codis de la plantilla per les cadenes que ha generat anteriorment obtenint un arxiu de configuració.

La informació de routing i d'ACL's IP és continguda a la plantilla dels switches de nivell 3 ( GS-4020 i ES-4124).

A la figura 6.2 es pot veure un diagrama que il·lustra el funcionament del programa.

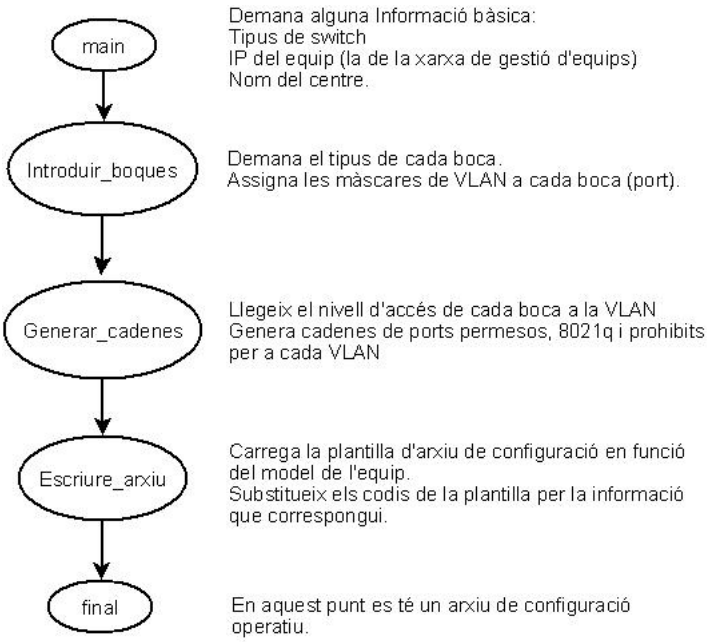



Figura 6.2: Diagrama de flux programa swgen.

Les característiques de l'arxiu de configuració són les següents:

1. Configura els ports acceptats a cada VLAN per cada tipus de boca (port) i activa si és necessari 802.1q.

2. Configura la IP de gestió.

3. Activa Spanning-Tree a totes les boques.

4. Als equips amb capacitat de routing configura les IP's de cada LAN i genera la taula de rutes.

5. Als equips amb capacitat de routing defineix les regles de control d'accés . Veure taules 6.1 i 6.2 pel detall de les regles que s'han implementat. Aquestes regles corresponen a la especificació definida al capítol 5.

| Origen | Destí | Xarxa Origen | Xarxa Destí | Acció |
|---|---|---|---|---|
| Alumnes | Professors | 192.168.0.0/16 | 10.1.0.0/16 | Denegar |
| Professors | Alumnes | 10.1.0.0/16 | 192.168.0.0/16 | Denegar |
| Alumnes | DocentWIFI | 192.168.0.0/16 | 10.3.0.0/16 | Denegar |
| DocentWIFI | Alumnes | 10.3.0.0/16 | 192.168.0.0/16 | Denegar |
| Alumnes | Eduroam | 192.168.0.0/16 | 10.4.0.0/16 | Denegar |
| Eduroam | Alumnes | 10.4.0.0/16 | 192.168.0.0/16 | Denegar |
| Alumnes | Gestió | 192.168.0.0/16 | 10.6.0.0/16 | Denegar |
| Gestió | Alumnes | 10.6.0.0/16 | 192.168.0.0/16 | Denegar |
| Alumnes | Servidors | 192.168.0.0/16 | 10.5.0.0/16 | Denegar |
| Servidors | Alumnes | 10.5.0.0/16 | 192.168.0.0/16 | Denegar |
| Servidor Alumnes | Servidors | 192.168.0.100/32 | 10.5.0.0/16 | Acceptar |
| Servidors | Servidor Alumnes | 10.5.0.0/16 | 192.168.0.100/32 | Acceptar |
| Alumnes | PAS | 192.168.0.0/16 | 10.2.0.0/16 | Denegar |
| PAS | Alumnes | 10.2.0.0/16 | 192.168.0.0/16 | Denegar |
| Professors | DocentWIFI | 10.1.0.0/16 | 10.3.0.0/16 | Denegar |
| DocentWIFI | Professors | 10.3.0.0/16 | 10.1.0.0/16 | Denegar |
| Professors | Eduroam | 10.1.0.0/16 | 10.4.0.0/16 | Denegar |
| Eduroam | Professors | 10.4.0.0/16 | 10.1.0.0/16 | Denegar |
| Professors | Gestió | 10.1.0.0/16 | 10.6.0.0/16 | Denegar |
| Gestió | Professors | 10.6.0.0/16 | 10.1.0.0/16 | Denegar |
| Professors | Servidors | 10.1.0.0/16 | 10.5.0.0/16 | Denegar |
| Servidors | Professors | 10.5.0.0/16 | 10.1.0.0/16 | Denegar |
| Professors | PAS | 10.1.0.0/16 | 10.2.0.0/16 | Denegar |
| PAS | Professors | 10.2.0.0/16 | 10.1.0.0/16 | Denegar |
| Servidor Profes | Servidors | 10.1.0.100/32 | 10.5.0.0/16 | Acceptar |
| Servidors | Servidor Profes | 10.5.0.0/16 | 10.1.0.100/32 | Acceptar |
| Docent WIFI | Eduroam | 10.3.0.0/16 | 10.4.0.0/16 | Denegar |
| Eduroam | Docent WIFI | 10.4.0.0/16 | 10.3.0.0/16 | Denegar |
| Docent WIFI | Gestió | 10.3.0.0/16 | 10.6.0.0/16 | Denegar |
| Gestió | Docent WIFI | 10.6.0.0/16 | 10.3.0.0/16 | Denegar |
| Docent WIFI | Servidors | 10.3.0.0/16 | 10.5.0.0/16 | Denegar |
| Servidors | Docent WIFI | 10.5.0.0/16 | 10.3.0.0/16 | Denegar |
| Docent WIFI | Servidor Profes | 10.3.0.0/16 | 10.1.0.100/32 | Acceptar |
| ServidorProfes | Docent WIFI | 10.1.0.100/32 | 10.3.0.0/16 | Acceptar |
| Docent WIFI | PAS | 10.3.0.0/16 | 10.2.0.0/16 | Denegar |
| PAS | Docent WIFI | 10.2.0.0/16 | 10.3.0.0/16 | Denegar |

Taula 6.1: Regles de control d'accés ACL's 1

| Origen | Destí | Xarxa Origen | Xarxa Destí | Acció |
|---|---|---|---|---|
| Eduroam | Gestió | 10.4.0.0/16 | 10.6.0.0/16 | Denegar |
| Gestió | Eduroam | 10.6.0.0/16 | 10.4.0.0/16 | Denegar |
| Eduroam | Servidors | 10.4.0.0/16 | 10.5.0.0/16 | Denegar |
| Servidors | Eduroam | 10.5.0.0/16 | 10.4.0.0/16 | Denegar |
| Eduroam | PAS | 10.4.0.0/16 | 10.2.0.0/16 | Denegar |
| PAS | Eduroam | 10.2.0.0/16 | 10.4.0.0/16 | Denegar |
| Gestió | Servidors | 10.6.0.0/16 | 10.5.0.0/16 | Denegar |
| Servidors | Gestió | 10.5.0.0/16 | 10.6.0.0/16 | Denegar |
| Gestió | PAS | 10.6.0.0/16 | 10.2.0.0/16 | Denegar |
| PAS | Gestió | 10.2.0.0/16 | 10.6.0.0/16 | Denegar |
| Servidors | PAS | 10.5.0.0/16 | 10.2.0.0/16 | Denegar |
| PAS | Servidors | 10.2.0.0/16 | 10.5.0.0/16 | Denegar |

Taula 6.2: Regles de control d'accés ACL's 2

El funcionament del programa és simple, consta dels passos següents.

1. A la línia de comandes introduir : swgen "nom de l'arxiu a generar".
2. Introduir el tipus de switch, la IP de gestió de l'equip i el nom del centre.
3. Introduir el tipus de cada boca (port).

Un cop es té l'arxiu generat es pot procedir a carregar-lo a l'equip. Consultar Apèndix 8.6.3.

A l'apèndix 8.5 es poden veure exemples d'arxius generats pel programa.

### 6.1.6 Configuració punts d'accés sense fils.

Per a la configuració dels punts d'accés sense fils veure el manual de l'apèndix 8.6.1

## 6.2 Configuració dels servidors.

Per a la millor comprensió de la implementació, es farà una introducció completa a la arquitectura emprada. Com es va veure a l'apartat de xarxa , la comunicació amb el servidor mestre només és permesa als altres dos servidors. Seguidament es mostrarà l'arquitectura del sistema de servidors diferenciant entre les parts del sistema :

- Base de dades LDAP : Descriu la estructura de la base de dades LDAP i la forma en que es distribueix pels diferents servidors.
- Autenticació d'usuaris : Descriu con s'autenticaran usuaris tant des d'estacions Windows XP com Linux.
- Compartició d'arxius en xarxa : Descriu quins sistemes d'arxius s'exportaran i amb quin protocol.
- Configuració dels diferents servidors : Descriu les característiques de la configuració dels servidors implicats en la validació d'usuaris i la exportació d'arxius.
- Configuració del Proxy : Descriu les característiques de la configuració de l'equip Proxy/Firewall.

### 6.2.1 Base de dades LDAP.

Com es pot veure a la figura 6.3. Els tres servidors es comuniquen mitjançant connexions xifrades amb TLS. La base de dades mestra de tot el centre es troba al servidor mestre. Els esclaus (professors i alumnes) sincronitzen el seu arbre LDAP amb el mestre. Com a mesura de seguretat l'arbre mestre s'ha dividit de tal forma que tant usuaris, dominis SAMBA, UIDs i altra informació relacionada siguin totalment independents.

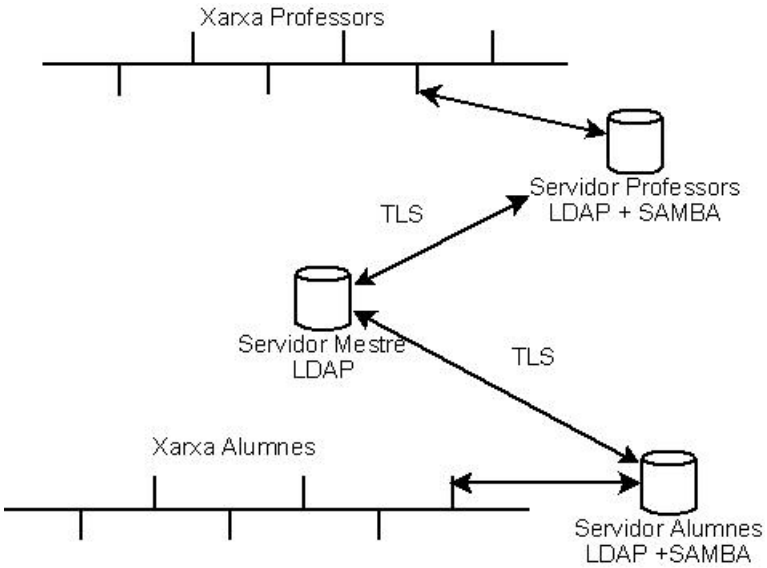



Figura 6.3: Estructura de servidors.

#### 6.2.1.1 Arbre LDAP.

A la figura 6.4 es pot veure l'estructura de l'arbre LDAP del servidor mestre. El núvol Dades domini X (Alumnes o Professors) significa que allí es guarda la informació del domini SAMBA corresponent i dividida en unitats organitzatives es guarda la informació d'usuaris, grups, equips, informació relativa a les UIDs i GIDs assignades als usuaris,etc. És a dir, tota la necessària per l'autenticació d'usuaris,grups i màquines en cada domini.

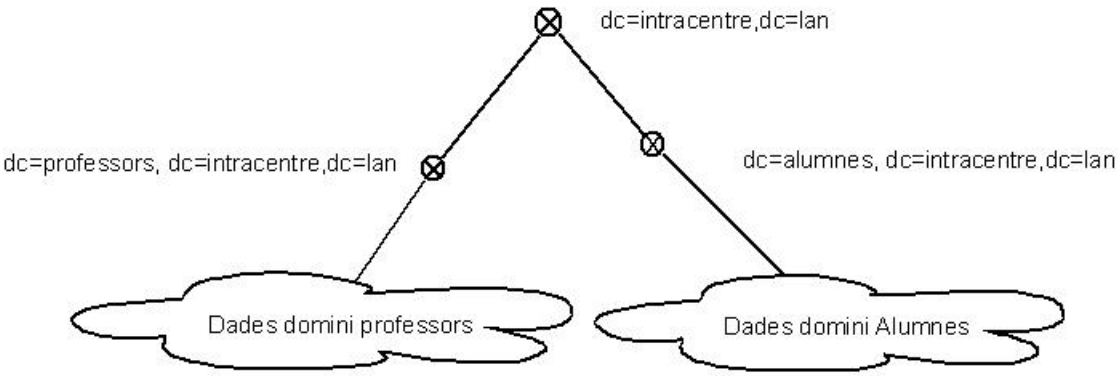



Figura 6.4: LDAP Master

A la figura 6.5 es pot veure l'estructura de l'arbre LDAP del servidor d'alumnes. Per aconseguir aquesta divisió s'han creat tres usuaris administradors diferents, un amb drets per llegir i modificar tot l'arbre, un amb dret per llegir i modificar la branca dc=alumnes... i amb prohibició total d'accés a la branca dc=professors... i el tercer administrador pot accedir a dc=professors i no a dc=alumnes. Aquestos usuaris es creen per necessitats de configuració de SAMBA i del client d'autenticació LDAP( veure arxiu de configuració slapd.conf i esquelet.ldiff dels servidors per detalls). Aquesta configuració és mes segura ja que si es compromet un dels servidors secundaris no s'obté dades suficients per accedir a la informació de l'altra branca de LDAP.

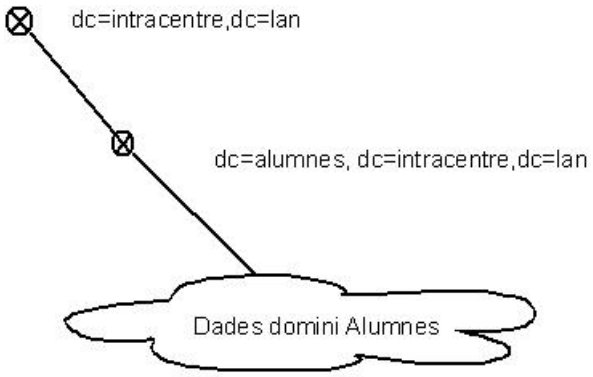



Figura 6.5: LDAP Alumnes

A la figura 6.6 es pot veure l'estructura de l'arbre LDAP del servidor de professors. Aquest subarbre té característiques similars al subarbre d'alumnes.

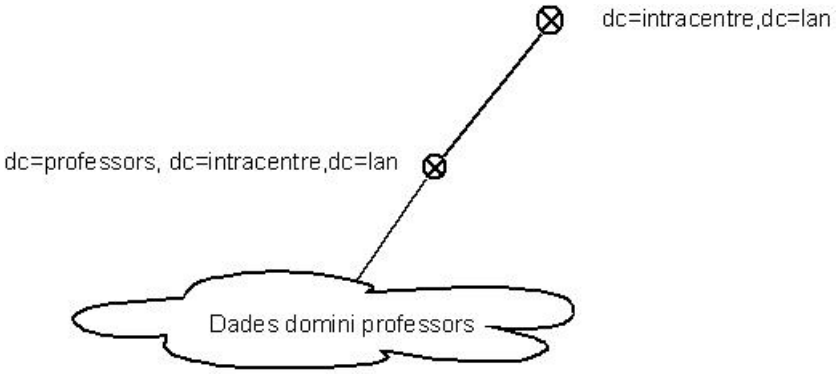



Figura 6.6: LDAP Professors

### 6.2.2 Autenticació d'usuaris.

#### 6.2.2.1 Autenticació en clients Windows XP.

Un cop s'ha vist la forma en que s'emmagatzemaran les dades d'autenticació d'usuaris és moment de veure la forma en que s'autenticaran els usuaris.

Per a l'autenticació dels equips Windows XP ja s'ha parlat de l'autenticació SAMBA. A la figura 6.7 es pot veure un esquema de com els servidors validaran usuaris en equips Windows XP. En aquest esquema s'observa que els clients s'autentifiquen mitjançant NTLMv2 amb el servidor SAMBA i que les dades que necessita el servidor SAMBA per validar són obtingudes de LDAP.

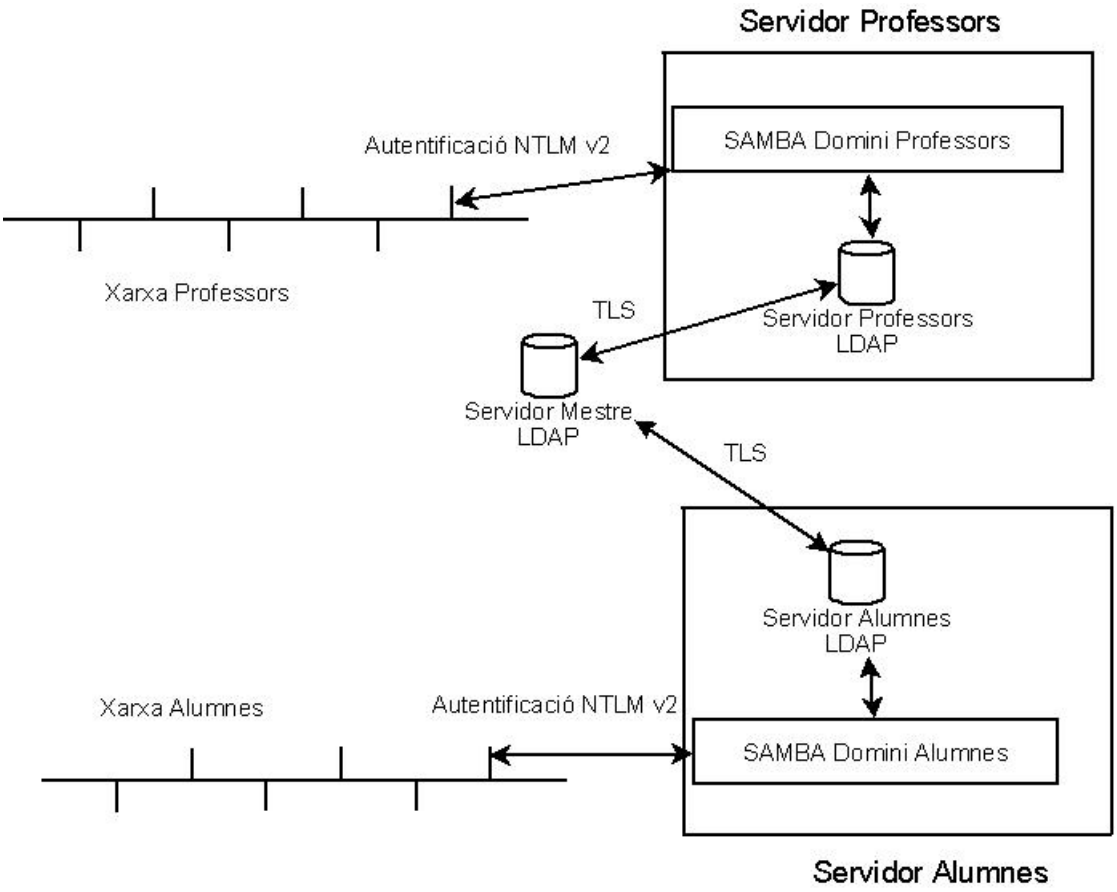



Figura 6.7: Esquema autenticació SAMBA.

Per a que un usuari es pugui identificar en el domini primer s'ha de seguir un procés que consisteix en l'intercanvi segur de claus de 128 bits entre el servidor i el client. Aquest procés és definit per Microsoft com procés d'addició al domini. Les claus criptogràfiques per a la validació s'intercanvien xifrades amb la contrasenya del administrador (el seu hash MD4) i el diagrama de flux d'aquest procés es pot veure a la figura 6.10, hauria de ser auto-explicatiu i comprèn el procés d'intercanvi de claus, i l'inserció en la base de dades LDAP d'una entrada per a la màquina on es guardaran les claus.

- SMBLDAPTools.

La utilitat SMBLDAPTools és formada per un conjunt de scripts Perl que permeten afegir i modificar informació administrativa rellevant per a l'autenticació en SAMBA (Windows XP) i en LDAP (Linux).Es configura per

modificar les dades conforme a l'arquitectura de la figura 6.8, és a dir SMBLDAPTools pot comunicar (Xifrat TLS) amb el servidor LDAP master per modificar informació. Aquesta informació actualitzada es propaga al LDAP esclau que és el que llegeix SAMBA. A la vegada SAMBA també pot cridar a comandes SMBLDAPTools per a actualitzar informació.

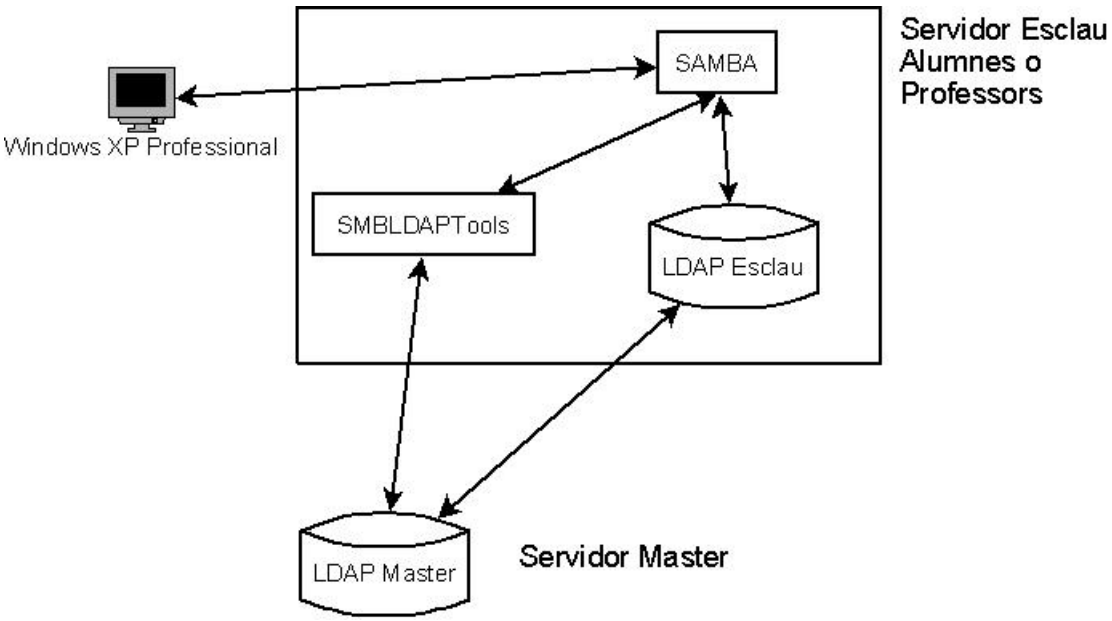



Figura 6.8: Connexió SMBLDAPTools.

L'autenticació de SAMBA és NTLMv2 , els detalls dels algorismes criptogràfics i de xarxa s'han vist anteriorment. Al diagrama de la figura 6.9 es veu el funcionament de NTLMv2 en la implementació feta en aquest treball.

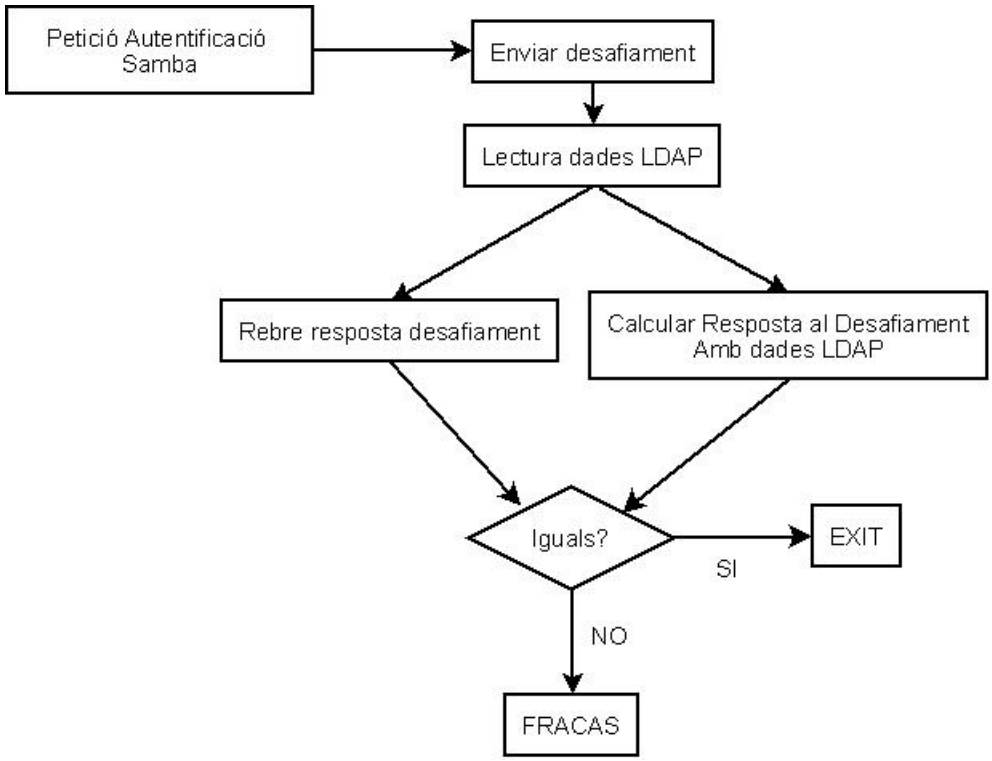



Figura 6.9: Autenticació NTLMV2

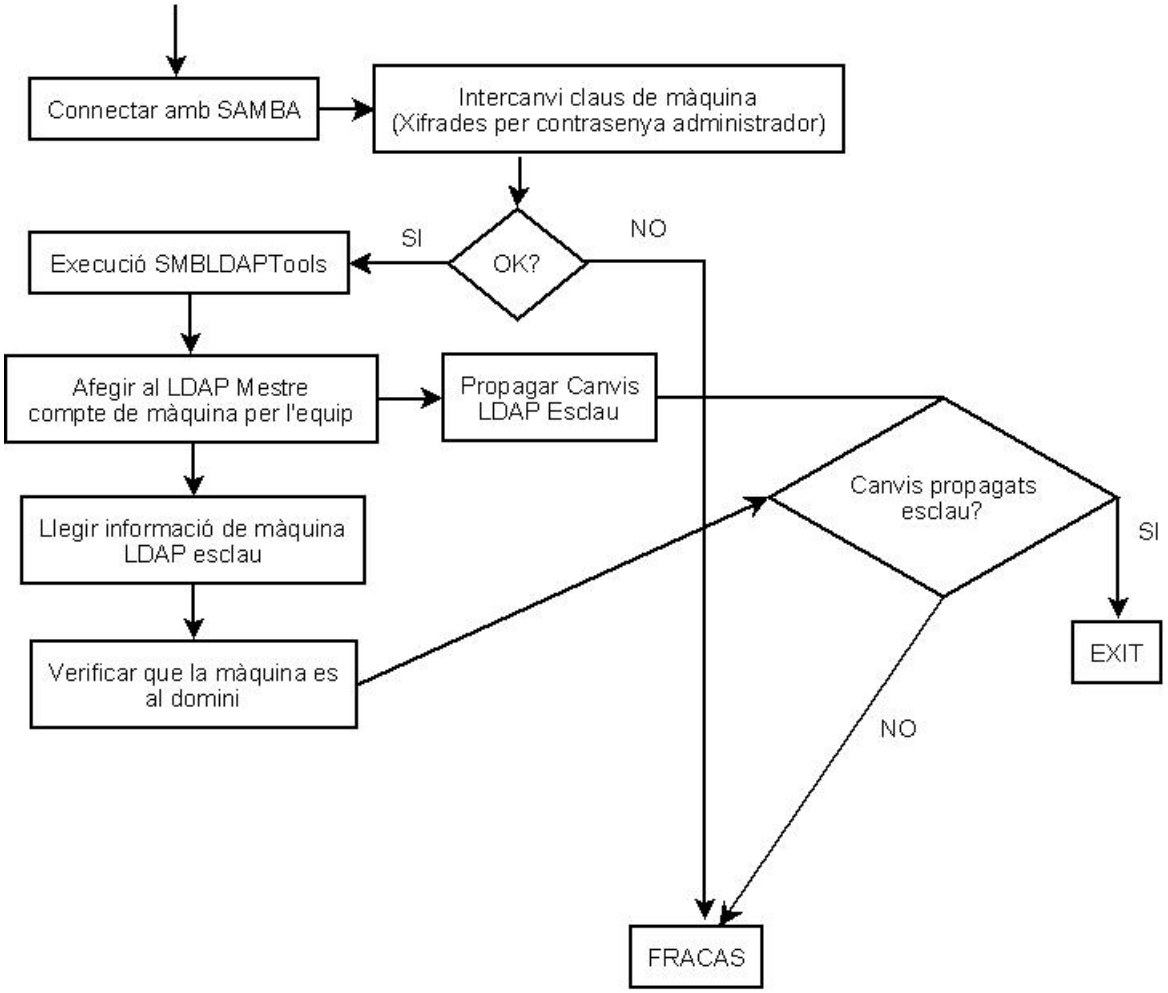



Figura 6.10: Diagrama de flux d'addició al domini.

Un cop la màquina es acceptada al domini, el procés de validació de usuaris i màquines en Windows funciona segons el diagrama de flux de la figura 6.11.

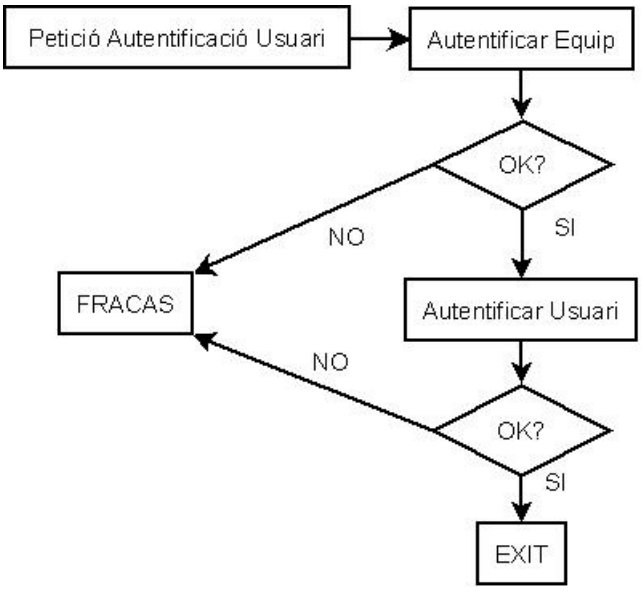



Figura 6.11: Diagrama de flux. Autenticació clients WindowsXP.

#### 6.2.2.2 Autenticació en Linux

La validació en clients Linux, es farà mitjançant LDAP+TLS. Els clients es validaran seguint l'esquema de la figura 6.12. La validació es fa directament contra LDAP, els clients s'autentifiquen contra els LDAP esclaus. Es fa servir el mòdul pam_ldap per l'autenticació dels clients.

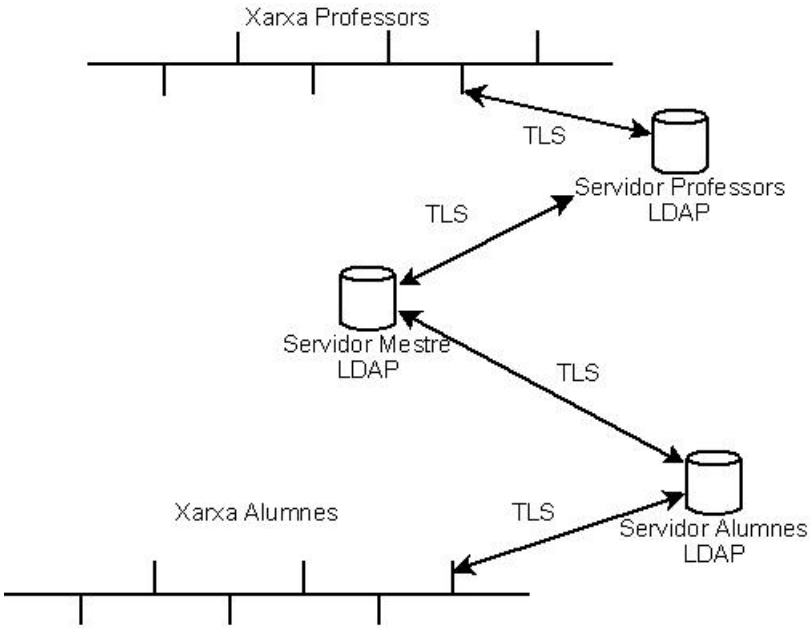



Figura 6.12: Esquema autenticació Linux.

El diagrama de flux de la operació d'autenticació contra LDAP és a la figura 6.13. L'usuari envia el seu nom de login corresponent al dn="nom_usuari",dc=X,dc=intracentre, dc=lan i la contrasenya en clar. L'intercanvi és protegit per un túnel TLS.
Si és vàlid atorga accés, si no el refusa.

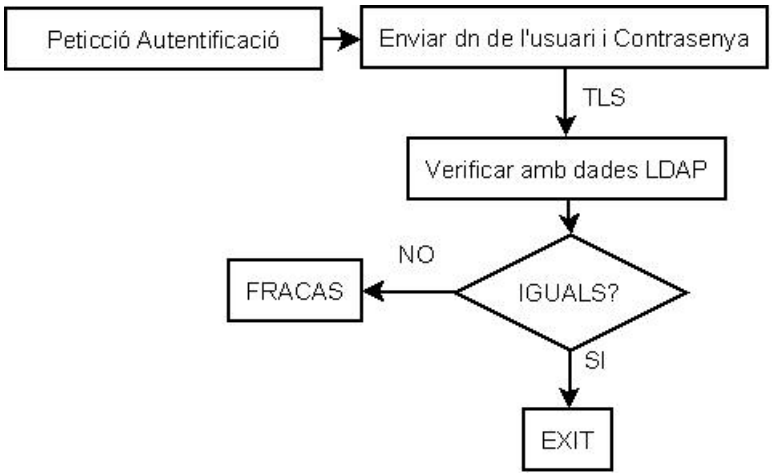



Figura 6.13: Diagrama d'autenticació Linux.

### 6.2.3 Compartició d'arxius en xarxa.

Es configurarà SAMBA per a que exporti els directoris "home" de cada usuari.

### 6.2.4 Configuració dels diferents servidors.

Tot seguit es dona informació de la configuració dels diferents servidors que intervenen en la validació d'usuaris i en la exportació d'arxius.

#### 6.2.4.1 Master

El servidor Master (mestre) és l'encarregat de mantenir una còpia de tot l'arbre LDAP (com ja s'ha vist), s'autentifica de manera local, es a dir els usuaris LDAP no es poden validar en aquest servidor. Això és una mesura de seguretat per a protegir el master, si algú té accés a un compte d'usuari LDAP no podrà fer login al master amb aquest i això comptant que hagi burlat la protecció de ACL's IP. Les característiques principals d'aquest servidor son :

- Ubicació : Xarxa de servidors.
- IP : 10.5.0.100/16 Gateway : 10.5.0.1
- Nom : master.intracentre.lan
- Certificat de servidor : master.crt i master.key (signats per cacert.pem)
- Serveis que corre : LDAP sobre TLS, manté una copia total de l'arbre LDAP.

El sistema operatiu sobre el que corre és Ubuntu server 7.10, aquesta distribució està optimitzada per a servidor, S'ha d'instal·lar el paquet "slapd" mitjançant la comanda" "apt-get install". Un cop instal·lats els paquets cal posar en marxa el servidor LDAP.

Per més detalls de la configuració consultar l'apèndix 8.1 on es troba la descripció dels arxius de configuració que s'han de modificar per a que el sistema funcioni segons la especificació.

Un cop modificats els arxius cal afegir al LDAP l'arxiu "esquelet.ldiff" mitjançant la comanda "slapadd". També caldrà crear certificats pels servidors. En aquest treball s'adjunten junt amb la resta d'arxius de configuració els certificats generats per a fer les proves. Per a més informació sobre la generació de certificats consultar [GENCERT] a la bibliografia. Un cop fet es reinicia el dimoni "slapd".

En aquest punt es té ja el servidor funcionant.

#### 6.2.4.2 Alumnes

El servidor d'alumnes és l'encarregat de validar els usuaris en la xarxa d'alumnes. A més exporta els directoris home dels usuaris per a que aquestos tinguin servei de dades centralitzat. Obté el subarbre LDAP d'alumnes del servidor mestre i manté una còpia de només lectura d'aquest. Les seves principals característiques son :

- Ubicació : Xarxa d'alumnes.
- IP : 192.168.0.100/16 Gateway : 192.168.0.1
- Nom : servalum.intracentre.lan
- Certificat de servidor : servalum.crt i servalum.key
- Serveis que corre. Són els següents.

1. LDAP : Corre un servidor LDAP que sincronitza el subarbre dc=alumnes, dc=intracentre,dc=lan amb el LDAP mestre.
2. SAMBA : Corre un servidor SAMBA com a controlador de domini pel domini "alumnes". A més exporta els directoris "home" dels usuaris a les màquines client Windows XP de forma automàtica. Per exportar a màquines Linux cal fer servir el mòdul "pam_mount".
3. SMBLDAPTools : No és un servei de xarxa pròpiament dit, sinó una sèrie de utilitats que permeten dur a terme operacions bàsiques d'administració : donar d'alta i baixa usuaris, grups, màquines, canviar contrasenyes de Windows i Linux. Les comandes bàsiques són :

- smbldap-useradd : Dona d'alta usuaris i màquines.
- smbldap-groupadd : Dona d'alta grups.
- smbldap-userdel : Dona de baixa usuaris i màquines.
- smbldap-groupdel : Dona de baixa grups
- smbldap-passwd : Canvia el password (SAMBA i UNIX).
- smbldap-usermod : Modifica dades d'usuari o maquina.
- smbldap-groupmod : Modifica dades de grups.

La configuració actual del servidor permet utilitzar aquestes eines en línia de comandes per a l'administració del sistema. A més SAMBA fa algunes crides a aquestes utilitats per a la gestió des de màquines Windows. Les màquines Windows XP es poden afegir al domini des dels quadres de diàleg corresponents en Windows. La contrasenya es pot canviar des de Windows XP i el canvi també afecta a la contrasenya de Linux. En aquest moments el canvi de contrasenyes des de Linux està vetat als usuaris (no poden executar directament SMBLDAPTools, només SAMBA o root ho poden fer.)

Per a la validació de clients Linux es pot consultar els arxius ldap.conf i auth_client_config.conf de l'apèndix 8.2. Aquestos arxius són els que tenen la informació bàsica de la que han de disposar els clients Linux.

Cal executar l'ordre "auth-client-config -a -p lac_ldap" per a configurar la validació correctament.

Per a més detalls de configuració veure els arxius de configuració a l'apèndix 8.2.

#### 6.2.4.3 Professors

El servidor de professors és molt semblant al d'alumnes, les configuracions son anàlogues. El servidor de professors manté una copia de només lectura del subarbre dc=professors,dc=intracentre,dc=lan. Les seves característiques son :

- Ubicació : Xarxa de professors.
- IP : 10.1.0.100/16 Gateway : 10.1.0.1
- Nom : servprof.intracentre.lan
- Certificat de servidor : servprof.crt i servprof.key
- Serveis que corre:

1. LDAP : Corre un servidor LDAP que sincronitza el subarbre dc=professors, dc=intracentre,dc=lan amb el LDAP mestre.
2. SAMBA : Corre un servidor SAMBA com a controlador de domini pel domini "professors". A més exporta els directoris "home" dels usuaris a les màquines client Windows XP de forma automàtica. Per exportar a màquines Linux cal fer servir el mòdul "pam_mount".
3. SMBLDAPTools : Ja s'ha parlat anteriorment a 6.2.4.

Per a la validació de clients Linux es pot consultar els arxius ldap.conf i auth_client_config.conf del l'apèndix 8.3. Aquestos arxius són els que tenen la informació bàsica de la que han de disposar els clients Linux.

Per a més detalls de configuració veure els arxius de configuració a l'apèndix 8.3.

### 6.2.5 Configuració del Proxy.

S'escull la distribució de Linux ClarkConnect Comunity edition 4.1 aquesta distribució és basada en RedHat i conté totes les aplicacions necessàries per a la realització de les funcions per a les que és destinat.

#### 6.2.5.1 Serveis que ofereix :

- Dans Guardian : Filtra els continguts de les pàgines web consultades, és capaç de reconèixer el contingut en base a assignar un pes específic a cada paraula i comptar-les. En cas que es superi el llindar denega l'accés. Pot també denegar l'accés a dominis sencers, permetre totalment dominis o negar la descàrrega en funció de la extensió de l'arxiu. També compta amb una àmplia col·lecció de "llistes negres" que engloben gran part dels dominis que es coneix que contenen continguts prohibits. Aquestes llistes negres són temàtiques i permeten una àmplia configuració.

- Squid Proxy Server : Estableix una cache de disc per als fitxers descarregats d'Internet (HTTP). D'aquesta manera es millora la velocitat d'accés a Internet. Aquest servidor actua de forma transparent redirigint els paquets amb destí als ports 80 i 8080 automàticament al port del servidor proxy. Per aquest motiu no és necessari configurar les estacions de treball per accedir al proxy.

- Iptables amb mòdul IPP2P : Aquest mòdul fa servir algoritmes de reconeixement de patrons per a classificar els paquets IP que es sospita que han estat generats per aplicacions P2P i els denega selectivament. Aquesta característica pot fer que en rares ocasions falli alguna aplicació de xarxa legítima. En aquest cas revisar la configuració i desactivar el mòdul si és necessari. Iptables també pot restringir a nivell de port i de IP.

- Interfície Web de control sobre Apache Server : Aquesta interfície facilita en gran mesura la configuració de l'equip, tots els serveis dels que s'ha parlat són configurables a través d'aquesta interfície.

- NAT i Firewall : Configurats sobre iptables.

Per a més detalls veure els arxius de configuració a l'apèndix 8.4.

## 6.3 Configuració dels equips clients.

Es configuraran els equips de les xarxes de professors i d'alumnes per a que puguin accedir als serveis oferts a la xarxa.

### 6.3.1 Clients Windows XP.

#### 6.3.1.1 Instal·lació Sistema Operatiu

Es recomana reinstal·lar el sistema operatiu amb l'objectiu d'eliminar programes no necessaris o no desitjats.

#### 6.3.1.2 Instal·lació programes

Després de la instal·lació del sistema operatiu es procedirà a instal·lar els programes que es facin servir per a la docència.

#### 6.3.1.3 Addició al domini

Cal afegir la màquina al domini que correspongui en cada cas. Pot ser necessari consultar la documentació del sistema operatiu per obtenir informació de com es realitza aquest procés. En aquest treball s'ha inclòs una animació (veure CD adjunt /vídeos/domain/addomain.html) en la qual es veu tot aquest procés.

#### 6.3.1.4 Còpia de seguretat

És altament recomanable realitzar una còpia de seguretat complerta del sistema instal·lat per a poder restaura-lo a l'estat inicial en cas de problemes.

#### 6.3.1.5 Instal·lació del programa Deep Freeze

El programa Deep Freeze és una aplicació propietària comprada pel Departament d'Ensenyament que protegeix el disc revertint els canvis fets als arxius de disc a cada reinici. És recomanable instal·lar-la ja que allarga la vida útil del sistema i redueix en gran mesura la freqüència amb la qual s'ha de restaurar les còpies de seguretat.

### 6.3.2 Clients Linux

#### 6.3.2.1 Configuració de la validació

Per a la validació de clients cal modificar la configuració els mòduls d'autenticació PAM (*Plugable Authentication Modules*) per a la validació LDAP. La configuració exacta depèn de la distribució de Linux que es faci servir. Per a les distribucions Debian, Ubuntu (i altres basades en Debian) és suficient configurar el programa "auth-client-config" i modificar /etc/ldap.conf tal i com es pot veure a l'apèndix 8.2 per a equips de la xarxa d'alumnes i com a l'apèndix 8.3 per a equips de la xarxa de professors.

#### 6.3.2.2 Configuració pam_mount.

Es configurarà el programa "pam_mount" per a muntar automàticament el directori "home" de l'usuari mitjançant CIFS. Consultar la documentació del programa per a la configuració.

## 6.4 Mesures de Seguretat recomanades

Seguidament es donaran alguns consells per incrementar el grau de seguretat i fiabilitat del sistema.

#### 6.4.0.3 Seguretat física.

És imprescindible implantar polítiques de seguretat física. Algunes recomanacions fàcils de complir son:

1. Mantenir els servidors en habitacions tancades i assegurar-se que només les persones autoritzades poden obtenir la clau.

2. Tancar els armaris de comunicacions amb clau.

3. Connectar l'alimentació elèctrica dels equips a sistemes d'alimentació ininterrompuda per evitar danys als equips per fluctuacions de corrent elèctric.

4. Posar candaus que impedeixin obrir la caixa que conté la CPU a les estacions de treball.

#### 6.4.0.4 Confidencialitat i control d'accés.

Tot i que els mecanismes dels que disposa el sistema per protegir la informació i per al control d'accés són robustos poden perdre tota la seva efectivitat si no es segueixen les següents recomanacions :

1. Escollir contrasenyes llargues, aleatòries i que continguin números i caràcters especials. Cal pensar que encara que s'emprin mecanismes criptogràfics aquestos no serveixen de gaire si les claus que es fan servir (contrasenyes) són fàcils d'endevinar.

2. Protegir les estacions de treball adequadament : És recomana prohibir l'arrencada des de dispositius extraibles (CDROM, disquetera) i protegir la configuració de la BIOS (*Basic Input Output System*) amb contrasenya. D'aquesta manera s'evita que algú pugui arrencar un sistema operatiu en el que es té privilegis d'administrador i obtenir fàcilment informació que li permeti obtenir accés no autoritzat al sistema. També s'evita que s'alterin les estacions per a la col·locació de programes espia (capturadors de teclat, etc.).

#### 6.4.0.5 Integritat de dades.

Per millorar la integritat de les dades es recomanen les següents actuacions :

1. Fer servir sistemes RAID 1 o 5 per a l'emmagatzemament de dades .

2. Fer còpies de seguretat de forma freqüent. A ser possible diàries.

#### 6.4.0.6 Auditoria.

És recomanable revisar periòdicament els arxius de bitàcora del sistema. Per dur a terme un bon control dels continguts accedits des de la xarxa és necessari revisar freqüentment els informes que es poden consultar mitjançant la interfície web del proxy. Als vídeos del CD adjunt es pot veure un exemple de com generar aquestos informes.

## 6.5 Proves.

Es van efectuar les següents proves per verificar la correcta configuració del sistema :

- Prova de ping de xarxa : Es va verificar la connectivitat entre les xarxes del projecte. A la figura següent es pot veure un esquema de la xarxa de proves que es va muntar. El programa script de proves i la sortida del programa es pot trobar al CD (/proves/provaping).

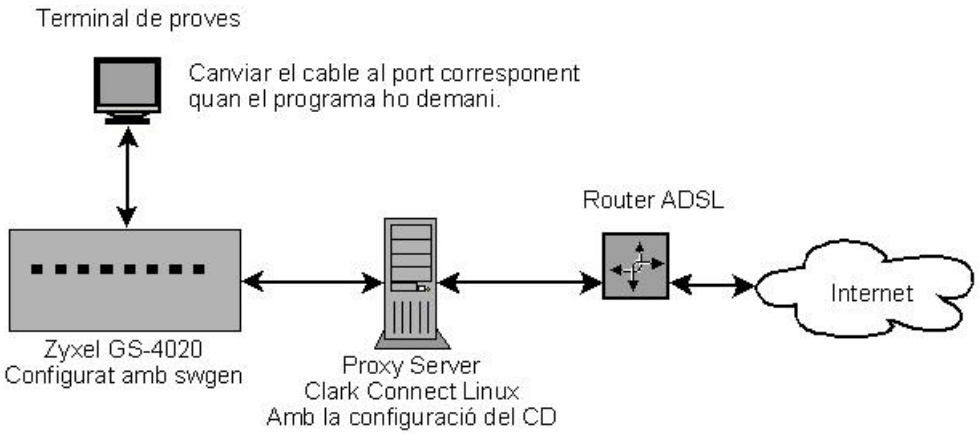



Figura 6.14: Esquema de xarxa de proves construïda.

- Prova d'addició massiva d'usuaris i estimació de cache RAM : Es van afegir 1000 usuaris amb la comanda :

```
#for i in ‘seq 1 1000‘ do ; smbldap-useradd -a -m -c prova $i;
                                done
```

Es va verificar la mida de la base de dades resultant per fer una estimació de la memòria requerida per establir una cache de RAM que donés el màxim rendiment. Després de calcular que cada usuari ocupa 21 KB d'espai en disc es recomana que la cache sigui del doble 42KB per usuari, d'aquesta manera és segur que la base de dades es pot mantenir en memòria i millorar el rendiment.

- Proves de funcionament del Proxy : Es va comprovar que el proxy efectivament bloquejava continguts prohibits i que es podien canviar els criteris de prohibició. Veure els vídeos adjunts (/videos/proxy).

- Prova de millora de cabal del Proxy : Es va fer servir la comanda `time wget -r -l 2 es.tldp.org` . Aquesta comanda es va executar dues vegades seguides per a que d'aquesta manera la segona vegada gran part de les dades fossin a la cache. La primera va atorgar un cabal de

4,29 Mbps, la segona com ja era al proxy va atorgar 21,24 Mbps. El Proxy de proves corria sobre màquina virtual, així que és possible que en màquines més potents i corrent nativament amb accés a disc a baix nivell s'incrementi encara més la millora.

- Proves de addició al domini : Es va verificar que les estacions Windows XP s'afegissin al domini correctament. Veure els vídeos del CD adjunt (/videos/domini).
- Proves de validació d'usuaris : Es va verificar que els usuaris es poguessin validar tant en Linux com en Windows. Veure els vídeos del CD Adjunt (/videos/domini).

## 6.6 Viabilitat econòmica del projecte.

Tot seguit s'avaluarà la viabilitat de la implantació del sistema. S'han calculat les despeses en funció dels següents conceptes :

- Obtenció del programari : Tot el programari és de lliure distribució i es pot obtenir lliure de càrrec. L'únic programa que té una llicència més restrictiva és el gestor de continguts DansGuardian. La llicència però permet expressament als centres educatius fer ús del programa sense haver de pagar. Així doncs el cost de llicència dels programes de servidor és 0 €.
- Estimació de cost de material : L'equipament de xarxa no té cap cost addicional, ja que es troba instal·lat. Els servidors es poden reciclar fent servir els equips servidor que ja té el centre en dotació. Si es preveu un gran volum de treball (200+ usuaris simultanis) és recomanable comprar els nous equips servidors. Segons es pot veure a l'apèndix cada servidor té uns requeriments recomanats per a altes càrregues de treball. Tot seguit es pot veure una taula que reflexa el cost aproximat de materials segons els requeriments recomanats de l'apèndix.

| Servidor Master | 600 € |
|---|---|
| Servidor Alumnes (Raid 5 SATA) | 2500 € |
| Servidor Professors | 700 € |
| Servidor Proxy | 800 € |
| Total | 4600 € |

Taula 6.3: Pressupost de Materials

Com es pot observar el cost és alt, però possiblement només centres molt grans requeriran la compra d'aquestos servidors. Tenint en compte que el número d'alumnes i la quantitat de grups del centre és el criteri principal d'assignació pressupostàriaés previsible que en centres grans (més de 2000 alumnes) això suposi entre un 1 i un 3 % del pressupost total anual del centre. Els centres amb nombre més petit d'usuaris poden reciclar ordinadors de dotació que ja tinguin.

- Estimació cost ma d'obra : Tenint les configuracions i les utilitats que es donen hauria de ser possible implantar el sistema de forma ràpida i fàcil. Es pot recórrer a tècnics del servei preventiu per a que instal·lin els servidors i la xarxa durant les visites del servei preventiu. D'aquesta manera no suposa cost addicional al centre.

- Conclusions : La instal·lació i posada en marxa dels servidors i la xarxa es considera viable. Pot ser implantada gairebé a cost nul. Encara que si els requeriments són grans la xifra pugui oscilar entre 4000 i 5000 €. Es de esperar que l'impacte pressupostari sigui mínim al tractar-se de centres grans amb amplis recursos. Per aquestes raons es considera que el projecte és viable.

# Capítol 7

# Conclusions.

Després d'haver implementat el sistema i un cop provat, s'arriba a les següents conclusions:

1. S'ha aconseguit configurar un sistema d'autenticació segura.
2. S'han habilitat espais de disc per a ús personal.
3. S'ha aconseguit controlar efectivament el tràfic de la xarxa i els continguts.
4. El nou sistema hauria de ser més robust i personalitzat.
5. S'han escrit manuals d'implementació.
6. S'ha implementat un sistema funcional i s'ha provat amb èxit.
7. És possible millorar el sistema. Veure capítol sobre treball futur.

# Capítol 8

# Treball Futur

A continuació es proposen algunes possibles millores al sistema implementat.

La majoria d'aquestes ampliacions es poden realitzar també amb programari de lliure distribució i es poden configurar per validar usuaris mitjançant la infraestructura d'autenticació de la xarxa existent.

- Habilitar portal per intercanvi informació : ex. moodle amb validació LDAP, apache, PHP i MySQL.
- Creació de programa o script per donar d'alta automàticament els usuaris : Cal programar-lo des de zero.
- Establir quotes de disc pels usuaris : Configurar-ho al sistema, es validarà contra LDAP.
- Creació de servei de email: Ex. Postfix amb validació LDAP.

# Part II

# Apèndix :

# Capítol 9

# Arxius configuració

Es descriuran breument els arxius de configuració de cada servidor. Al començament de cada secció es dona el camí dels arxius de configuració de cada servidor dins el CD adjunt a la documentació.

## 9.1 Servidor master

Tot seguit es farà una breu explicació de les funcions de cada arxiu de configuració del servidor master. Aquestos arxius es poden consultar a : /configs/master/ en el CD adjunt.

### 9.1.1 Requeriments mínims

Els requeriments mínims per a aquest servidor no són molt grans. Pot servir un ordinador Pentium4 amb 256 MB de RAM. Es pot millorar el rendiment amb més memòria augmentant la mida de la cache de la base de dades de LDAP. La base de dades LDAP ocupa en disc 21 MB per cada 1000 usuaris, és de esperar que en memòria pugui ocupar més així que si:
$(21 * 1024)/1000 = 21$KB per usuari. Com que en memòria és possible que ocupi més s'aplica un factor de correcció del 200% i es requereix 42KB per usuari.Per un centre de 3000 usuaris cal doncs 3000*42 = 126 MB. Aquesta serà la mida de la caché en RAM així doncs amb els 256 MB de base la memòria recomanada per 3000 usuaris és de 512 MB (256+126 aproximat a la potència de dos). Avui en dia es poden comprar servidors de rack d'aquestes característiques per 400 € amb cache L2 de 4MB i memòries ràpides i múltiples nuclis que donarien un rendiment excel·lent en les consultes. El rendiment que es pot obtenir també pot trobar un coll d'ampolla en la connexió de xarxa, així que es recomana Gigabit Ethernet. Amb un ordinador

d'aquestes característiques es pot controlar un centre amb gran nombre de usuaris (3000+) i d'ordinadors clients (300+).

Centres amb pocs ordinadors i pocs usuaris poden reciclar algun servidor que compleixi els 256 MB de RAM.

### 9.1.2 LDAP

#### 9.1.2.1 /etc/ldap/slapd.conf

Aquest arxiu conté la configuració del servidor LDAP. S'ha modificat la informació de les ACL's i la relativa a la localització dels certificats x.509 per a complir amb la especificació. Es recomana generar nous certificats d'usuari, ja que els proporcionats són públics.Ha fet falta també afegir algunes opcions per a la replicació.

Si es vol és possible augmentar la cache de RAM per a màxim rendiment. Calcular la formula 42KB* #usuaris i substituir la X (Per defecte 2 MB) del paràmetre "dbconfig set_cachesize 0 X 0" per la xifra que ens doni.

#### 9.1.2.2 esquelet.ldiff

Conté la base de l'arbre LDAP i la informació relativa als tres usuaris administradors que fan possible la separació de dominis. Es recomana canviar les contrasenyes abans de carregar-lo al LDAP per motius de seguretat ja que aquest és un treball públic.

### 9.1.3 Xarxa

#### 9.1.3.1 /etc/network/interfaces

Aquest arxiu conté informació d'adreçament IP, màscares i encaminament.

### 9.1.4 Resolució de noms

#### 9.1.4.1 /etc/hosts

Conté les IPs de cada servidor. No es fa servir DNS.

#### 9.1.4.2 /etc/hostname

Conté el nom del servidor.

## 9.2 Servidor alumnes

### 9.2.1 Requeriments mínims

Són els mateixos que el servidor master. Recomanable el doble de RAM que el master i implementar RAID 1 o 5 per dotar de tolerància a fallides de disc. Si el nombre d'estacions és elevat és possible que es degradi el rendiment del servidor d'arxius. Comprar unitats de disc ràpides i una bona controladora RAID per hardware pot ser car (1000€-3000€) i només es recomana per a centres amb gran nombre d'estacions (200+) ja que milloraria molt el rendiment d'accés a fitxers en condicions d'alta càrrega. Si el subsistema de disc és prou ràpid es pot optar també per afegir una o més targetes Gigabit Ethernet i fer servir el protocol LACP (*Link Agregation Control Protocol*) per augmentar l'ample de banda de la connexió a xarxa del servidor i eliminar el coll d'ampolla. Aquestos requeriments recomanats són suficients per a centres amb gran nombre d'estacions i usuaris. Els centres amb menor número d'estacions poden optar per implementar RAID 1 per software per redundància de dades.

### 9.2.2 LDAP

Tot seguit es farà una breu explicació de les funcions de cada arxiu de configuració del servidor servalum. Aquestos arxius es poden consultar a : /configs/alumnes/ en el CD adjunt.

#### 9.2.2.1 /etc/ldap/ldap.conf

Aquest arxiu conté la informació necessària pel client LDAP+TLS.

#### 9.2.2.2 /etc/slapd.conf

Aquest arxiu conté la configuració del servidor LDAP.

#### 9.2.2.3 esquelet.ldiff

Conté la base de l'arbre LDAP.

### 9.2.3 Xarxa

#### 9.2.3.1 /etc/network/interfaces

Aquest arxiu conté informació d'adreçament IP, màscares i encaminament.

### 9.2.4 Resolució de noms

#### 9.2.4.1 /etc/hosts

Conté les IPs de cada servidor. No es fa servir DNS.

#### 9.2.4.2 /etc/hostname

Conté el nom del servidor.

### 9.2.5 SAMBA

#### 9.2.5.1 /etc/samba/smb.conf

Aquest arxiu conté la configuració del SAMBA. Les seves característiques principals són:

- Controlador principal del domini ALUMNES.
- Backend de dades : dc=alumnes,dc=intracentre,dc=lan
- Integració de smbldap-tools per a la modificació del LDAP.
- Exportació de directoris personals.

### 9.2.6 Autenticació

#### 9.2.6.1 /etc/auth-client-config/profile.d/ldap-auth-config

Aquest arxiu conté la informació necessària per modificar nsswitch.conf i els arxius de pam.d per a configurar l'autenticació d'usuaris i grups mitjançant LDAP. És necessari a totes les estacions Linux que hagin de validar usuaris de LDAP.

### 9.2.7 SMBLDAPTools

És una col·lecció de scripts programats en Perl que assisteixen les principals tasques d'administració del sistema.

#### 9.2.7.1 /etc/smbldap-tools/smbldap.conf

Conté la informació per connectar als servidors LDAP, inclosa la relativa als certificats criptogràfics per a TLS.

#### 9.2.7.2 /etc/smbldap-tools/smbldap.bind

Conté les credencials per accedir al LDAP.

## 9.3 Servidor professors

### 9.3.1 Requeriments mínims

Els mateixos que el servidor master. Recomanable RAID 1 per redundància de dades. No es necessiten unitats de disc especialment ràpides ja que el nombre d'estacions dedicades exclusivament a professorat sol ser menor.

### 9.3.2 LDAP

Tot seguit es farà una breu explicació de les funcions de cada arxiu de configuració del servidor servprof. Aquestos arxius es poden consultar a : /configs/professors/ en el CD adjunt.

#### 9.3.2.1 /etc/ldap/ldap.conf

Aquest arxiu conté la informació necessària pel client LDAP+TLS.

#### 9.3.2.2 /etc/slapd.conf

Aquest arxiu conté la configuració del servidor LDAP.

#### 9.3.2.3 esquelet.ldiff

Conté la base de l'arbre LDAP.

### 9.3.3 Xarxa

#### 9.3.3.1 /etc/network/interfaces

Aquest arxiu conté informació d'adreçament IP, màscares i encaminament.

### 9.3.4 Resolució de noms

#### 9.3.4.1 /etc/hosts

Conté les IPs de cada servidor. No es fa servir DNS.

#### 9.3.4.2 /etc/hostname

Conté el nom del servidor.

### 9.3.5 SAMBA

#### 9.3.5.1 /etc/samba/smb.conf

Aquest arxiu conté la configuració del SAMBA. Les seves característiques principals són:

- Controlador principal de domini : PROFESSORS
- Backend de dades : dc=professors,dc=intracentre,dc=lan
- Integració de smbldap-tools per a la modificació del LDAP.
- Exportació de directoris personals.

### 9.3.6 Autenticació

#### 9.3.6.1 /etc/auth-client-config/profile.d/ldap-auth-config

Aquest arxiu conté la informació necessària per modificar nsswitch.conf i els arxius de pam.d per a configurar l'autenticació d'usuaris i grups mitjançant LDAP. És necessari a totes les estacions Linux que hagin de validar usuari de LDAP.

### 9.3.7 SMBLDAPTools

És una col·lecció de scripts programats en Perl que assisteixen les principals tasques d'administració del sistema.

#### 9.3.7.1 /etc/smbldap-tools/smbldap.conf

Conté la informació per connectar als servidors LDAP, inclosa la relativa als certificats criptogràfics per a TLS.

#### 9.3.7.2 /etc/smbldap-tools/smbldap.bind

Conté les credencials per accedir al LDAP.

## 9.4 Servidor Proxy

### 9.4.1 Requeriments mínims

Tenint en compte que el filtrat de continguts és un procés CPU-intensiu cal que el proxy tingui un processador ràpid i prou memòria. Es recomana un mínim de 1 Gb de memòria i un processador Athlon64 3000+ , Pentium 4 2,4 GHz o superior. Processadors més ràpids i el doble de memòria asseguren un òptim rendiment.

No hi ha requeriments especial pel disc dur. Un disc SATA (*Serial ATA*) de 7200 rmp amb 16 MB de cache sol ser suficient.

### 9.4.2 Configuració del Proxy.

Al CD adjunt a la memòria (/configs/proxy ) es pot trobar un arxiu amb una configuració per defecte que habilita totes les funcions anteriors. Aquest arxiu es pot carregar mitjançant la interfície web del Proxy i d'aquesta manera es pot configurar el sistema sense tenir grans coneixements.

És necessari fer algunes modificacions :

- Permetre connexions sortints UDP al port 1814 (per defecte ja esta així).
- Configurar a l'apartat "Network" de la interfície web una tarja Ethernet com a "external" (amb DHCP) i una altra tarja com a "LAN" amb la IP 10.7.0.1/16.
- Habilitar les rutes modificant copiant l'arxiu /etc/rc3.d/S99local del CD.
- Cal també afegir a l'arxiu /etc/squid/squid.conf el següent:

acl our_networks src 192.168.0.0/16 10.1.0.2/16 10.2.0.2/16 10.3.0.2/16 10.4.0.2/16 10.5.0.2/16 10.7.0.2/16
http_access allow our_networks

## 9.5 Programa swgen

### 9.5.1 Codi

El codi es pot consultar a l'arxiu swgen_pfc.tar.gz del CD adjunt. Consta de les següents parts.

#### 9.5.1.1 swgen.h

Definició de prototips de funció.

#### 9.5.1.2 swgen.c

Implementació de les funcions.

#### 9.5.1.3 Plantilla GS-4024. (GS-4024.log)

Conté la configuració base fixa i uns codis que serveixen al programa per fer la substitució dels paràmetres que poden variar.

#### 9.5.1.4 Plantilla ES-4124. (ES-4124.log)

Conté la configuració base fixa i uns codis que serveixen al programa per fer la substitució dels paràmetres que poden variar.

#### 9.5.1.5 Plantilla ES-2024. (ES-2024.log)

Conté la configuració base fixa i uns codis que serveixen al programa per fer la substitució dels paràmetres que poden variar.(ES-2024.log)

### 9.5.2 Exemples

Es donen alguns exemples d'arxius generats pel programa. Veure dins el paquet comprimit del programa els arxius que comencen per "exemple".

## 9.6 Manuals Equips

### 9.6.1 Configuració des de zero dels punts d'accés D-Link DWL-2200AP

#### 9.6.1.1 Configuració de la xarxa sense fils

Connectem amb un navegador a la IP del punt d'accés, per defecte 192.168.0.50.

Introduir username "admin" i sense password.

Prémer el botó "Wireless".

Arribem a la pantalla de la figura 8.1, aquesta cal emplenar-la exactament com es veu a la imatge :

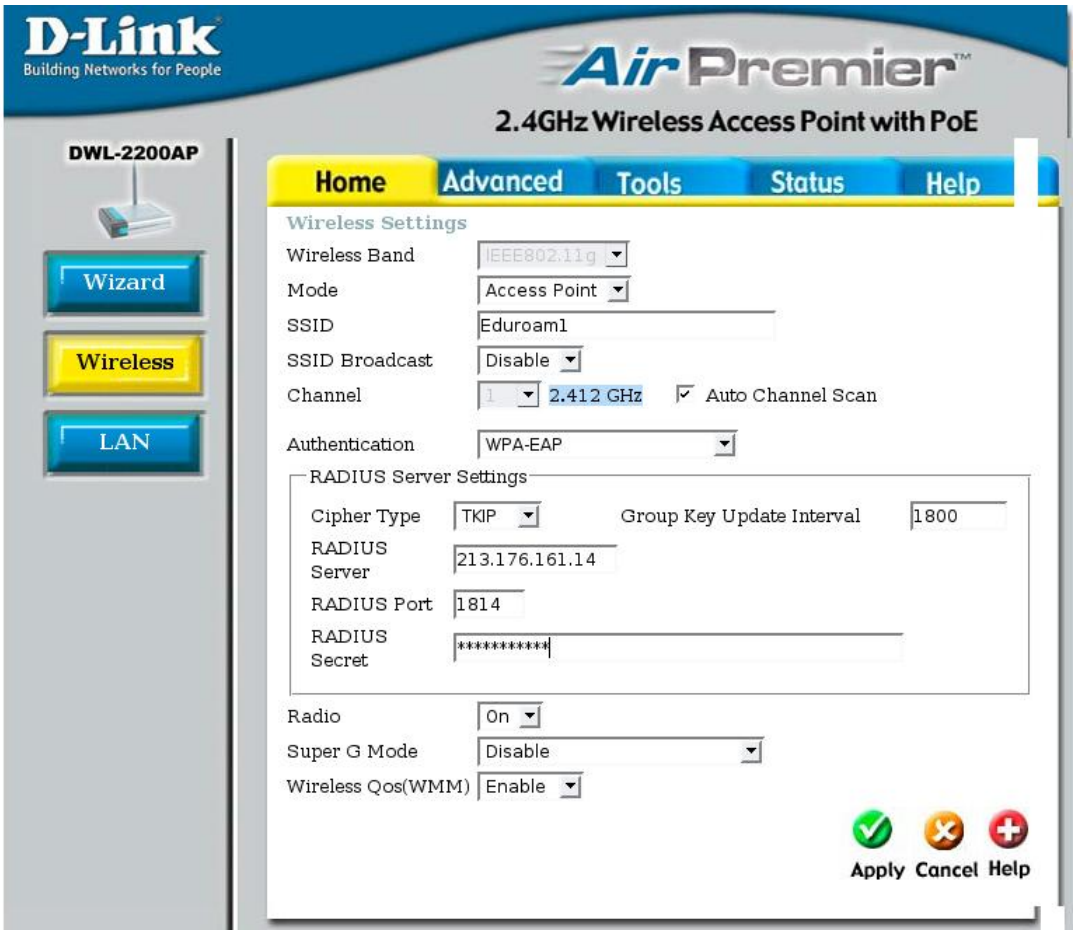



Figura 9.1: Configuració wireless.

Aquest punt d'accés detecta la banda amb menys interferència i assigna la banda automàticament. Això és especialment útil quan el centre té interferències externes o altres punts d'accés que no són del projecte heura. Permet que la banda de freqüència s'ajusti automàticament a les bandes amb menys soroll electromagnètic, aconseguint així la millor qualitat de senyal possible. En cas de voler configurar manualment el canal cal dins de la mateixa pantalla (veure figura 8.1) desactivar "Auto Channel Scan", desplegar la pestanya "Channel" i seleccionar el canal.

La contrasenya "RADIUS Secret" és ******* (consultar la documentació del Departament d'Educació).

Un cop emplenat premem el botó "Apply".

El punt d'accés farà un reinici

Un cop reiniciat anem a la pestanya "Advanced" i premem el botó "Multi-SSID".

Veurem la pantalla de la figura 8.2:

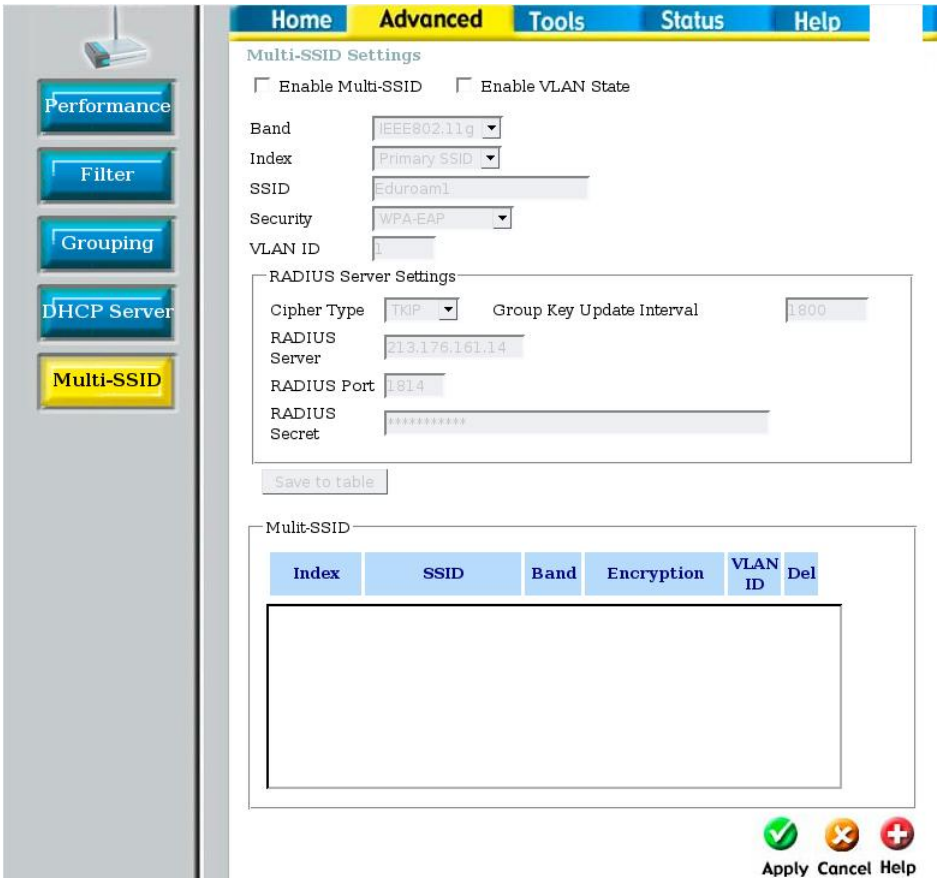



Figura 9.2: Configuració wireless MultiSSID

Cal marcar “Enable Multi-SSID” i “Enable VLAN State”.

Un cop fet això cal deixar la pantalla amb els valors exactes de la figura 8 .3.

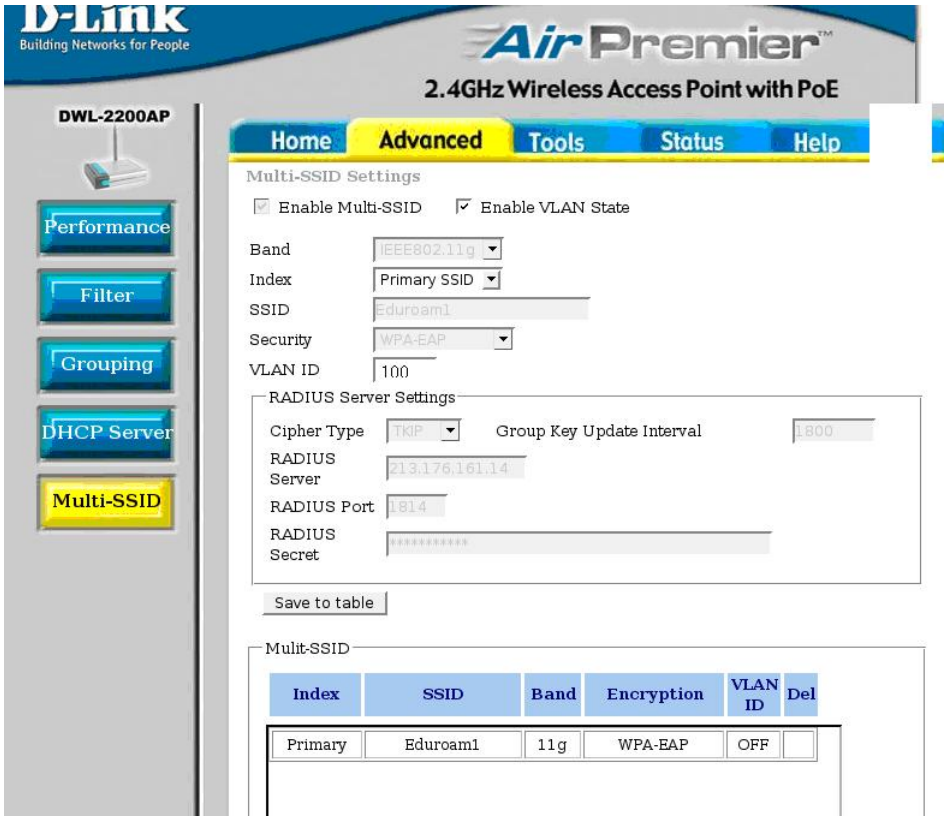



Figura 9.3: Configuració wireless MultiSSID primari

Premem el botó "Save to table". El motiu de posar la VLAN ID igual a 100 és per aconseguir que ningú pugui connectar al SSID primari. Com la VLAN 100 no existeix a la nostra configuració ni es defineix al switch, tots els paquets amb destí la VLAN 100 son descartats automàticament pel switch i d'aquesta manera s'impedeix la connexió. Tot això es fa per motius de seguretat, ja que només s'ha de poder connectar a "docent" i "eduroam".

La pantalla de la figura 8.4 també cal deixar-la tal i com es veu a la imatge .

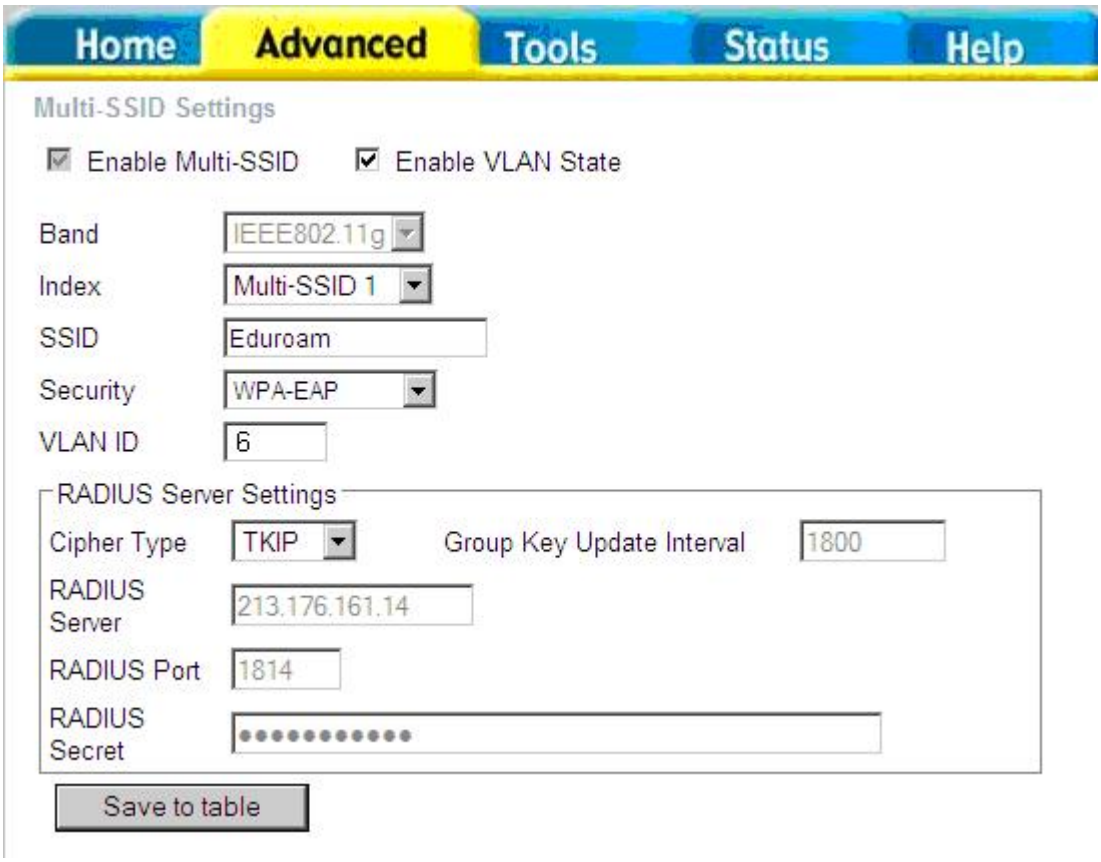



Figura 9.4: Configuració wireless eduroam

Tornem a prémer "Save to table".

Tornem a deixar les opcions de la pantalla de la figura 8.5 con es veu a la imatge.

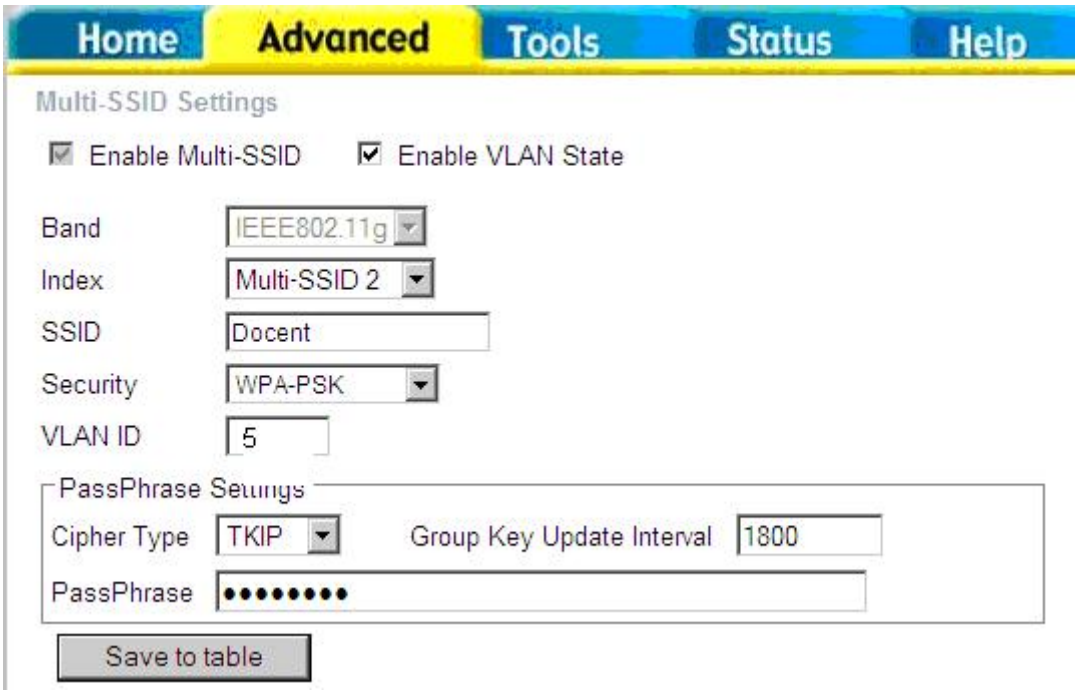



Figura 9.5: Configuració wireless docent

La contrasenya "PassPhrase" és la que es farà servir per connectar a la xarxa.

Tornem a prémer "Save to table".

Si tot ha anat bé a la part baixa de la pantalla veurem el següent.

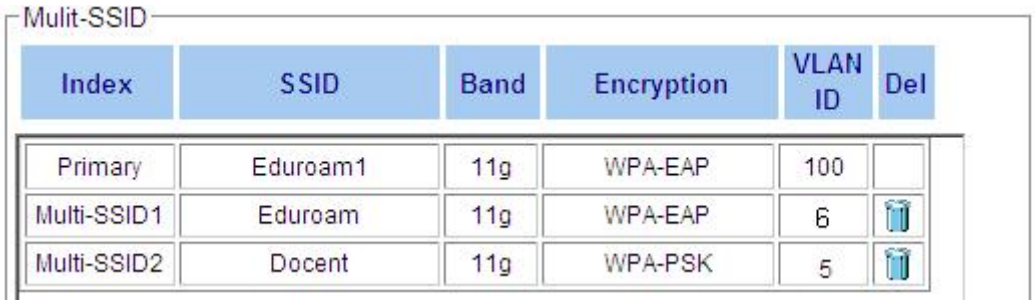



Figura 9.6: Configuració Wireless. Taula MultiSSID

Si la taula "Multi-SSID" ha quedat com es veu a la figura premem el botó "Apply".

#### 9.6.1.2 Canvi de clau de l'administrador.

Un cop fet això cal anar a la pestanya "Tools". Veurem la pantalla de la figura 8.7 :

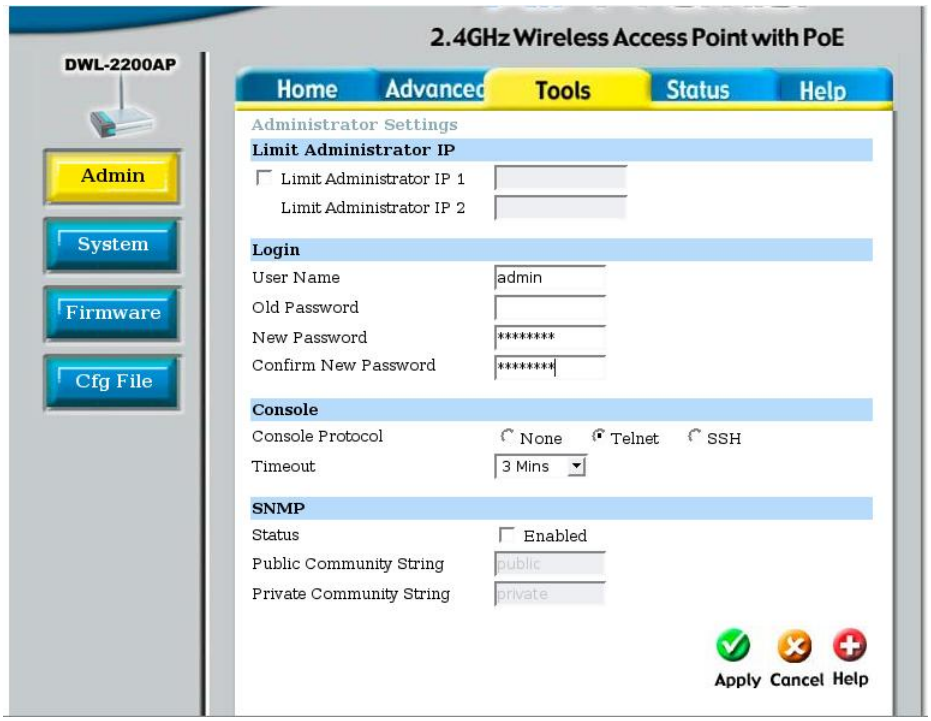



Figura 9.7: Configuració Wireless. Canvi contrasenya

Cal emplenar els camps "New Password" i "Confirm New Password" amb la contrasenya que es desitgi.

Després premem el botó "Apply".

#### 9.6.1.3 Canviar la IP del punt d'accés :

Dins aquesta pantalla de la figura 8.8 cal clickar al botó "LAN" .

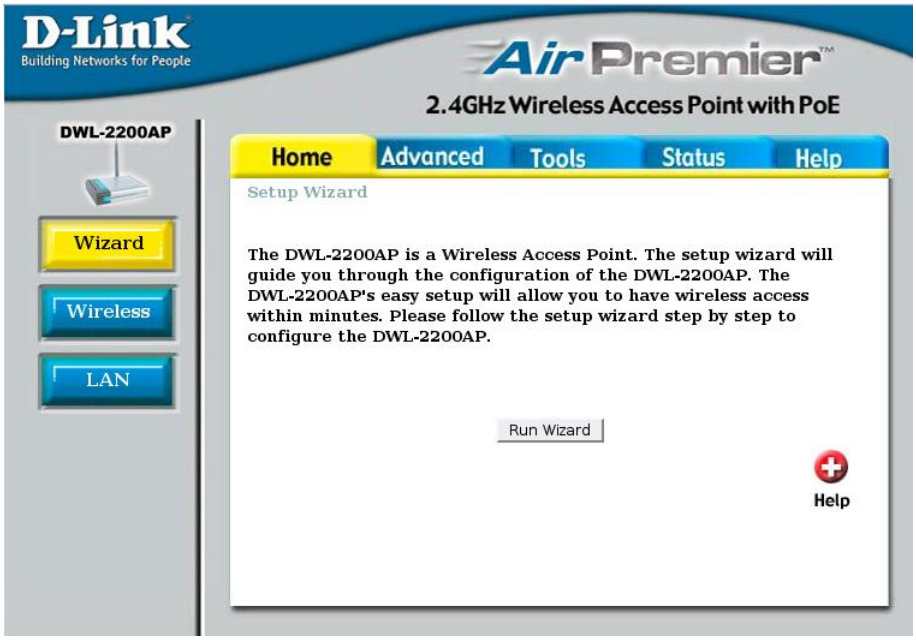



Figura 9.8: Configuració wireless. Canvi IP

Cal omplir els camps com s'indica :

Get IP From : Static (Manual)

Ip Address : 10.6.1.10-100 (Es pot fer servir altres IPs del rang)

Subnet Mask : 255.255.0.0

Default Gateway : 10.6.0.1

Premem botó "Apply"

El punt d'accés ja està llest i es pot connectar a una boca del switch configurada per a punts d'accés.

#### 9.6.1.4 Creació de l'arxiu de configuració.

Un cop dins la pàgina principal del punt d'accés seleccionen la pestanya "Tools" i dins d'aquesta seleccionem el botó "Cfg File".

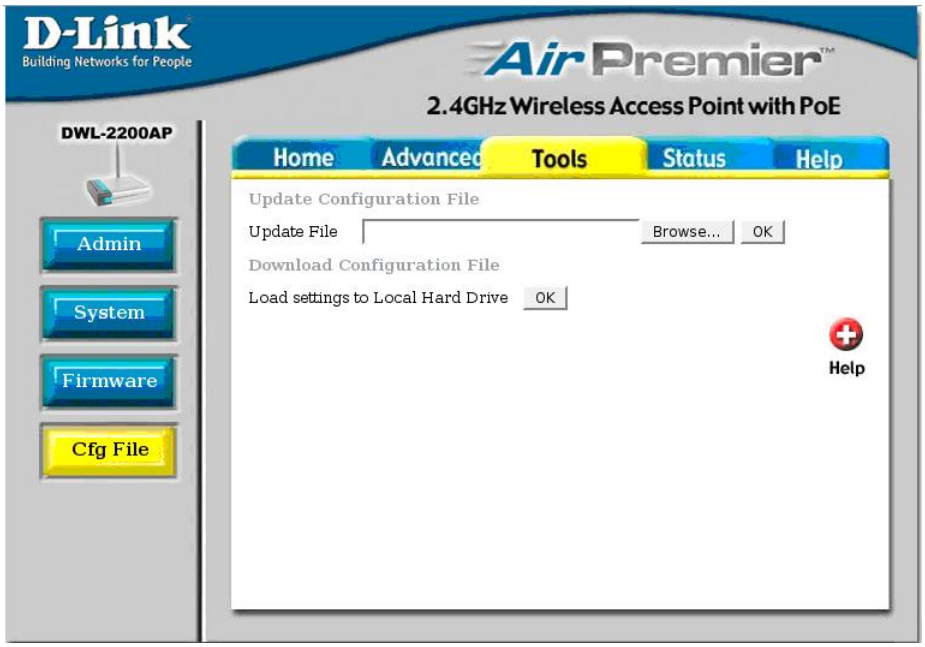



Figura 9.9: Configuració Wireless. Creació i restauració configuració.

Premem el boto "OK" Que hi ha al costat de "Load settings to Local Hard Drive". El navegador obrirà una descàrrega, l'arxiu descarregat és l'arxiu de configuració del punt d'accés.

#### 9.6.1.5 Restauració de l'arxiu de configuració.

No sempre serà necessari fer tota la configuració de forma manual, si disposem de l'arxiu de configuració del punt d'accés procedirem a restaurar-lo com es veu a continuació.

Procedirem a obrir una sessió al punt d'accés amb un navegador d'Internet com s'ha vist anteriorment.

Un cop dins la pàgina principal del punt d'accés seleccionen la pestanya "Tools" i dintre d'aquesta seleccionem el botó "Cfg File".

Premem el botó "Browse" i busquem al nostre ordinador l'arxiu de configuració. Un cop seleccionat premem el botó "OK".

Un cop fet això ja tenim configurat el punt d'accés. En aquest cas si que és possible que ens canviï la contrasenya, ja que en el cas dels punts d'accés la contrasenya es guarda al arxiu de configuració i canvia quan el restaurem.

### 9.6.2 SAI

Per a la configuració del SAI es pot optar per fer-ho mitjançant telnet o per port sèrie. En ambdós casos la interfície és similar. Com el SAI ve preconfigurat pel projecte Heura només serà necessari canviar-li l'adreça IP.

Els paràmetres per configurar amb el port sèrie son :

- Bits per segon : 9600
- Bits de dades : 8
- Paritat : Sense paritat.
- Bits de Parada : 1
- Control de flux : Sense control de flux

En aquesta pantalla cal prémer la tecla "ESC" i tot seguit la tecla "Enter" varies vegades fins que ens demani entrar el nom d'usuari.

Introduïm com a login "root" i com a password el que posa a la documentació del Departament d'Educació.

Apareixerà la pantalla següent:

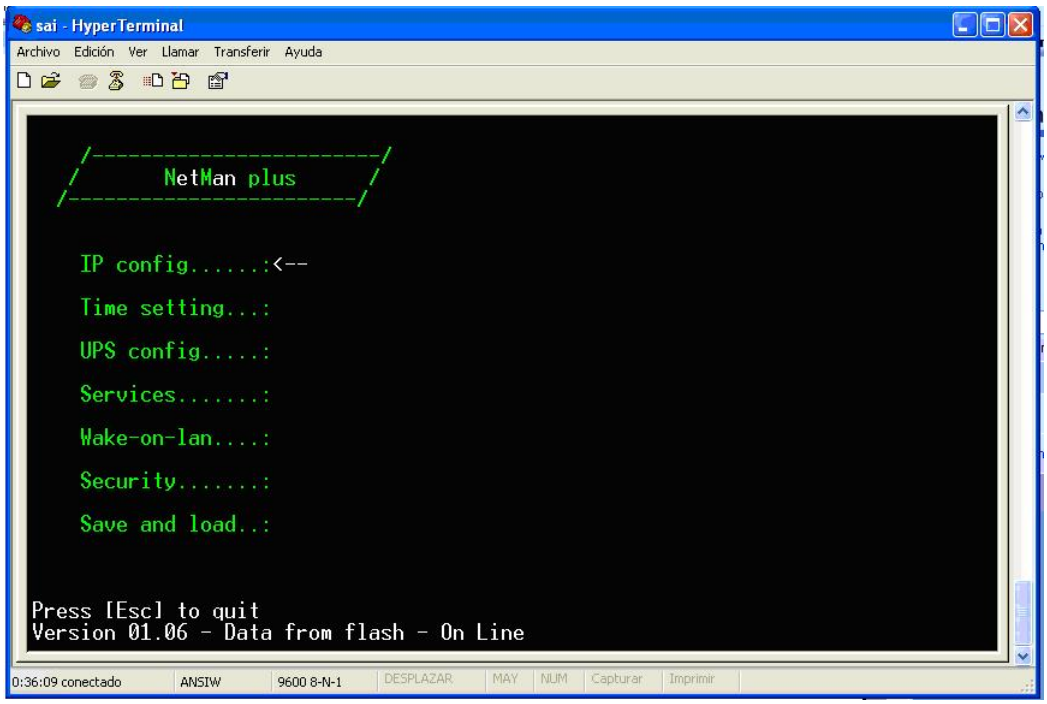



Figura 9.10: Pantalla inici de configuració del SAI.

Seleccionar IP config.
Es veurà la pantalla següent :

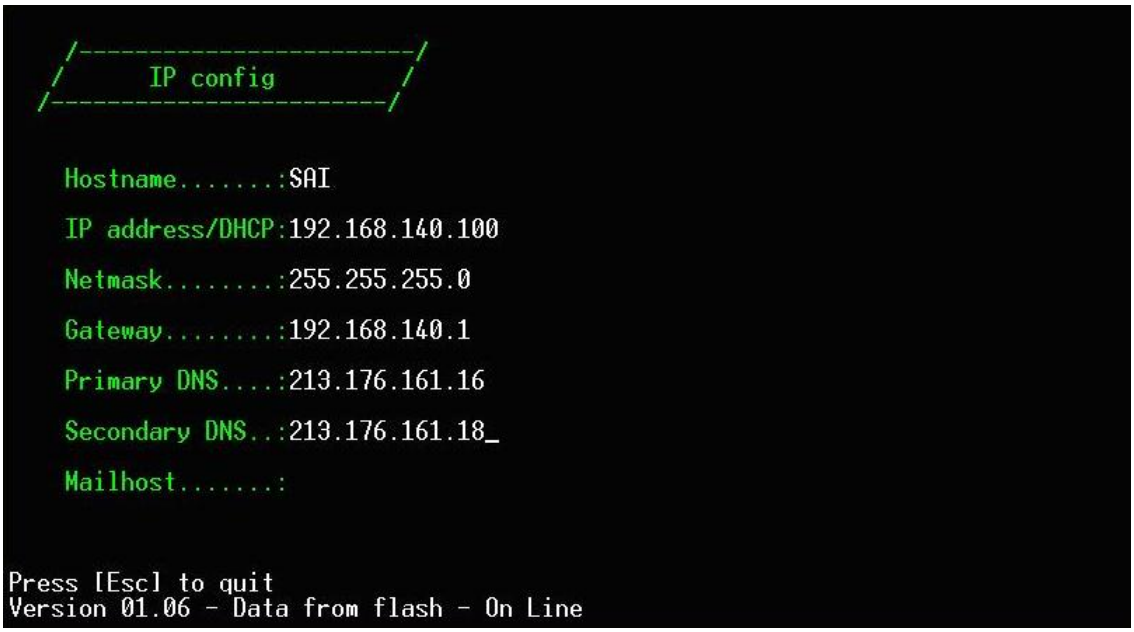



Figura 9.11: Pantalla de configuració IP.

En aquesta pantalla s'ha de substituir els següents valors existents :
IP address : 10.6.0.100
Netmask : 255.255.0.0
Gateway : 10.6.0.100
La resta de valors es queden igual.
Un cop modificats els valors, es guarda la configuració.
En aquest punt el SAI es troba configurat amb l'adreçament del sistema correcte. Caldrà també modificar la configuració dels programes de gestió SNMP que accedeixen al SAI per a que tinguin configurada la nova IP.

### 9.6.3 Bolcat de configuració al switch.

Per a realitzar un bolcat de configuració:

1. Connectar al switch : La configuració d'Heura està activa al centre, així que cal consultar en la documentació del projecte Heura que es lliura al centre. Un cop es coneix la IP de l'equip connectar-se mitjançant un navegador d'Internet.

2. Introduir nom d'usuari (admin) i password del equip
3. Seleccionem l'opció "Management" del menú esquerre.
4. Seleccionem l'opció "Maintenance", després "Restore Configuration"
5. Seleccionem el botó Examinar i triem el fitxer que desitgem restaurar (El generat per swgen per l'equip en qüestió).
6. Seleccionem l'opció Restore.
7. Un cop restaurada la contrasenya no varia ja que aquesta no és modificada per l'arxiu de configuració.
8. En aquest punt es recomana re iniciar l'equip.

# Bibliografia


[AXSTP] Apunts de Xarxes EPS 2005-6.pdf. Secció 4.2.4 Bucles

[AXVLN] Apunts de Xarxes EPS 2005-6.pdf. Secció 4.2.5 Lan virtuals

[TLSRFC] The TLS Protocol Version 1.0 (RFC2246)

[RSA1024] Adi Shamir, Eran Tromer, On the cost of factoring RSA-1024, RSA CryptoBytes, vol. 6 no. 2, 10-19, 2003

[LDAPP] LDAPv3 Protocol (RFC 2251)

[HMAC] HMAC: Keyed-Hashing for Message Authentication (RFC 2104)

[NTLMCRK] Cracking NTLMv2 Authentication. Security Friday

[SPEUI] Simson Garfinkel y Gene Spafford, O'REILLY Seguridad Practica en Unix e Internet 2a edició.

[SHARFC] US Secure Hash Algorithm 1 (SHA1) (RFC 3174)

[SLDUBHWT] SAMBA+LDAP Ubuntu Howto (http://ubuntuforums.org/showthread.php?t=640760)

[DOCSAMBA] Documentació del programari SAMBA (complet a www.samba.org). Pàgines de manual de *smbd*, *smb.conf, nmbd* (comanda *man).*

[DOCLDAP] Documentació del programari OpenLDAP (complet a www.openldap.org). Pàgines de manual de *ldap.conf*, *slapd.conf*, *slapd.* (comanda *man).*

[RFCX509] Internet X.509 Public Key Infrastructure (RFC2459).

[DOCOSSL] Documentació OpenSSL. (complet www.openssl.org).

[CENCERT] Generating x.509 certificates. *http://www.ipsec-howto.org/x595.html*